NetWitness® Platform

Version 12.5

NetWitness Respond User Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

September, 2024

Contents

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 automatically 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. 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.

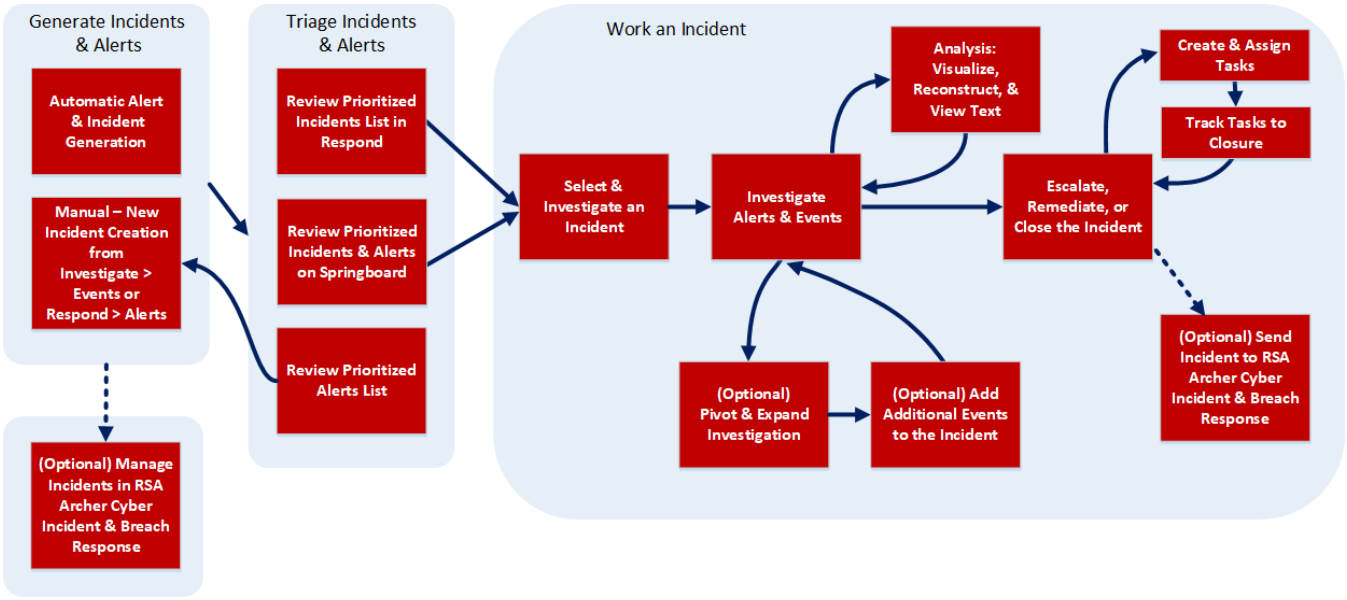
The stages in the NetWitness Respond process are:

- **Generate Incidents & Alerts**
  - Automatic Alert & Incident Generation
  - Manual - New Incident Creation from Investigate > Events or Respond > Alerts
  - (Optional) Manage Incidents in Archer Cyber Incident and Breach Response (If you manage incidents in Archer instead of in NetWitness Respond, the process ends here.)
- **Triage Incidents & Alerts**
  - Review Prioritized Incident List in Respond
  - Review Prioritized Incidents & Alerts on Springboard
  - Review Prioritized Alerts List
- **Work an Incident**
  - Select & Investigate Incident
  - Investigate Alerts & Events
    - Analysis: Visualize, Reconstruct, and View Text
    - (Optional) Pivot & Expand Investigation
    - (Optional) Add Additional Events to Incident

- Escalate, Remediate, or Close the Incident
  - Create & Assign Tasks
  - Track Tasks to Closure
  - (Optional) Send Incidents to Archer Cyber Incident & Breach Response. (In NetWitness version 11.2 and later, if Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response.)

NetWitness Respond Workflow

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



Responding to Incidents

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

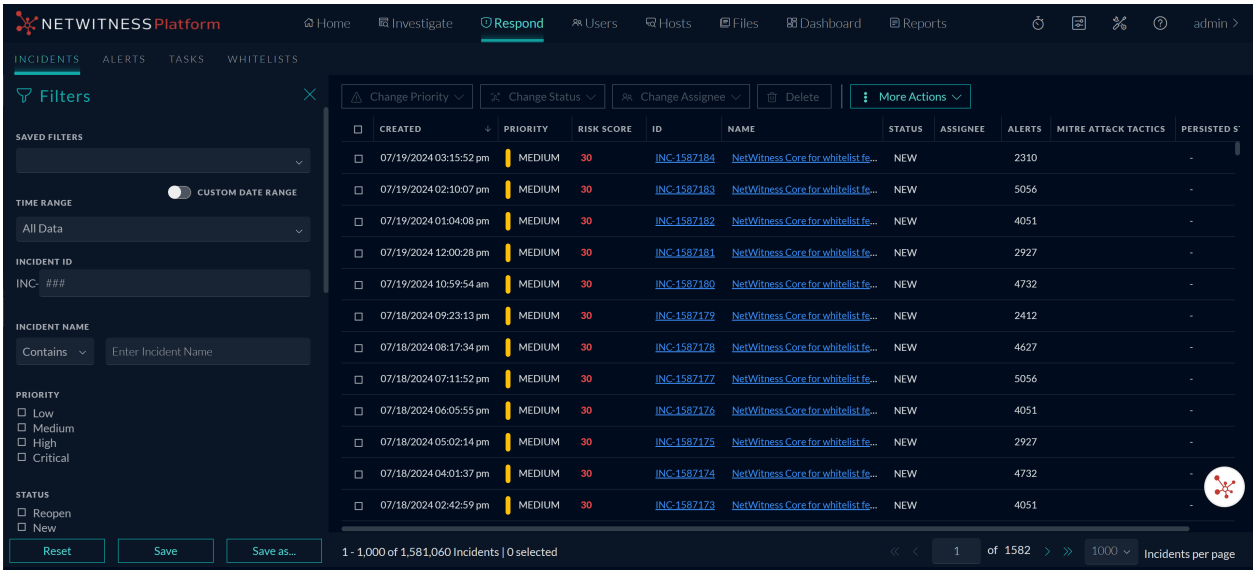
The **Respond** view is designed to help you quickly identify the ongoing issues in your network and work with other Analysts to quickly solve the issues.

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.

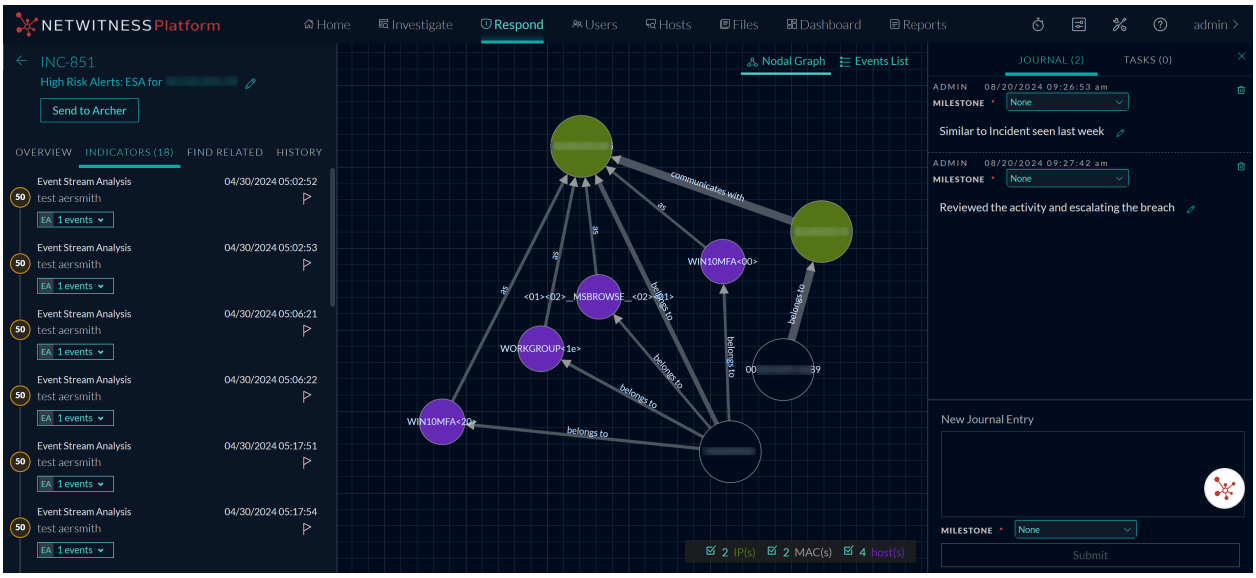
Within the Respond view, you can see Incidents, Alerts, and Tasks:

- **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 and create incidents from selected alerts.
- **Tasks**: Enables you to view and manage the complete list of tasks created for all incidents.

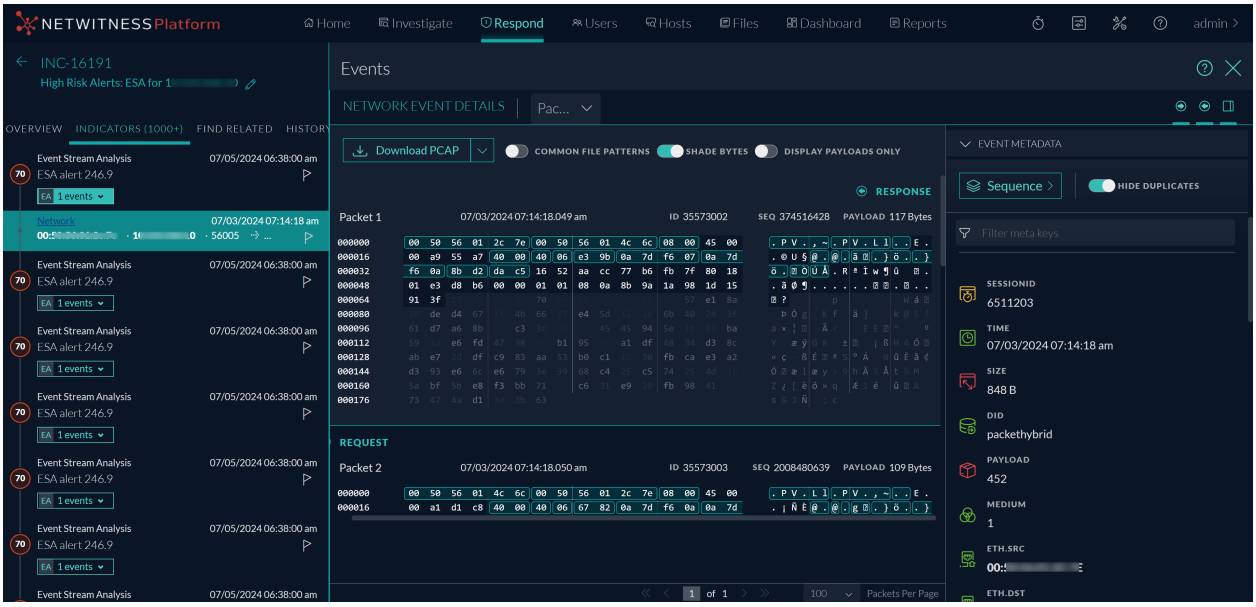
If you navigate to Respond > Incidents, you can see the Incidents List view and from there you can access the Incident Details view for a selected incident. These are the main views that you use to respond to incidents. The following figure shows the list of prioritized incidents in the **Incidents List**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



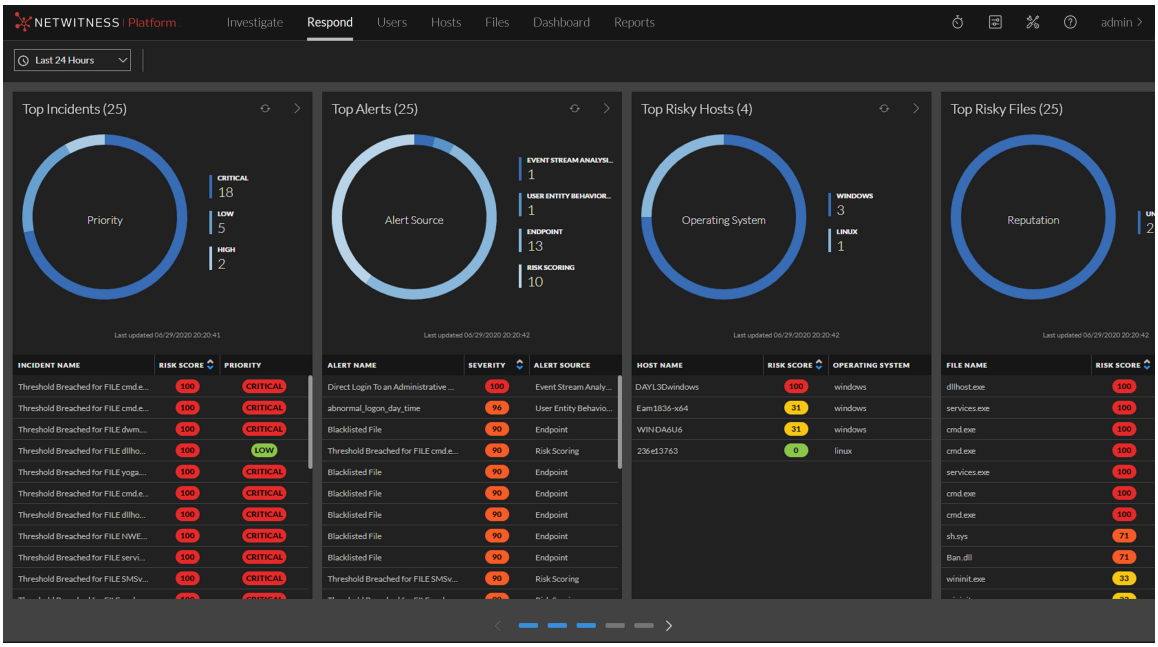
The next figure shows an example of details available in the **Incident Details** view.



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.



In NetWitness Version 11.4 and later, alerts and incidents are also displayed in the Springboard by default. Springboard is a landing page for analysts showing them all risks detected by the platform in a single place. For more information on the Springboard, see "Managing the Springboard" in the *NetWitness Platform Getting Started Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.



Respond Persist Data

The primary objective of this feature is to enable you to investigate events for a longer period of time. When investigating a set of alerts or events, it is important to have the assurance that the underlying data (raw and meta) will be available for both the length of time it takes to run the analysis, and for historical look up. From NetWitness Platform Version 11.6, you can persist events that are associated with particular incidents, thereby enabling you to view the incident in the future, regardless of its age. You can also add a new journal entry in the **JOURNAL** tab for the persisted events for future reference. The event data will always be available for viewing and reconstruction as long as the event is persisted, enabling you to easily refer back to details, even if the original event has rolled over from the NetWitness database.

Once you persist an event, the data is copied from the NetWitness database into a long term storage cache within the data source. You can persist or suspend persist events per incident or per alert within an incident or a specific event in an alert that belongs to an incident. The roll over in the NetWitness database does not impact the events that are already saved in the long term cache.

You can:

- You can persist or suspend persist events per incident or per alert within an incident or a specific event in an alert that belongs to an incident.
- Perform complete event reconstruction for persisted events even after the session is rolled over from the NetWitness database.

- Filter incidents which has persisted events.
- Suspend persist of all events associated with an incident, even if only a few events persisted in it.
- Remove all associated persisted events by deleting an alert or incident.

This topic contains the following basic Respond Persist Data procedures:

Customizing Respond Persist Data

The persisted events are saved in the directory `/var/netwitness/pin-<servicetype>`, by default. You can manually change the event storage location from the default directory to any other directory, as per the requirement. You can increase the storage space as per your requirement by performing an Network File System (NFS) mount. For more information on how to perform an NFS mount, see Configure the Destination Using NFS.

To customize the persist directory:

1. Go to **Admin** >**Services**.
The **Services** page appears.

2. From the **Filter** pull down menu, select the concentrator and the log decoder services.
The concentrator and log decoder are listed in the **Services** page.

3. Go to **Actions** > **View** > **Explore**.
The **Explore** page appears.

4. Go to **sdk** > **config** .

The **Configuration** page appears.

The following table provides information on the default values for each parameter that are configured in the **Configuration** page.

S.No	Parameter	Default Value
1.	Long Term Cache Behavior (pin.cache.behavior)	fail-on-new
2.	Long Term Cache Directory (pin.cache.dir)	/var/netwitness/pin-<serviceType>***
3.	Long Term Cache Size (pin.cache.size)	10 GB

2. [Optional]*** In the **Long Term Cache Directory (pin.cache.dir)**, enter the path of the custom directory where you want to save the persisted events, if you do not want to use the default location. The default path is `/var/netwitness/pin-S<serviceType>`.

Note: When you install NetWitness Platform for the first time or upgrade to the 11.6 version, the directories are pre-configured with default values.

Working with Incident Filters

You can filter incidents based on the persisted events.

To filter incidents:

1. Go to **Respond** > **INCIDENTS**.

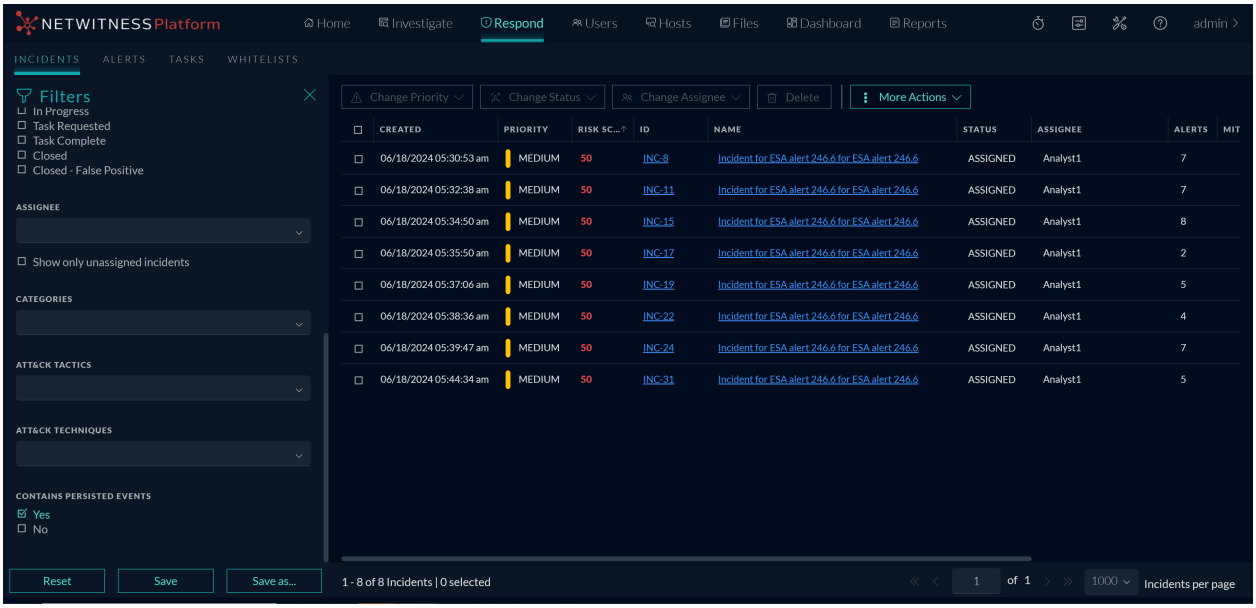
The **INCIDENT** page appears.

2. In the **FILTERS** tab, the **CONTAINS PERSISTED EVENTS** menu provides the filters to view incidents based on the persisted events.

a. Select **Yes** to view the incidents that contain persisted events.

b. Select **No** to view the incidents that do not contain persisted events.

For more information on working with filters, see Filter the Incident List.

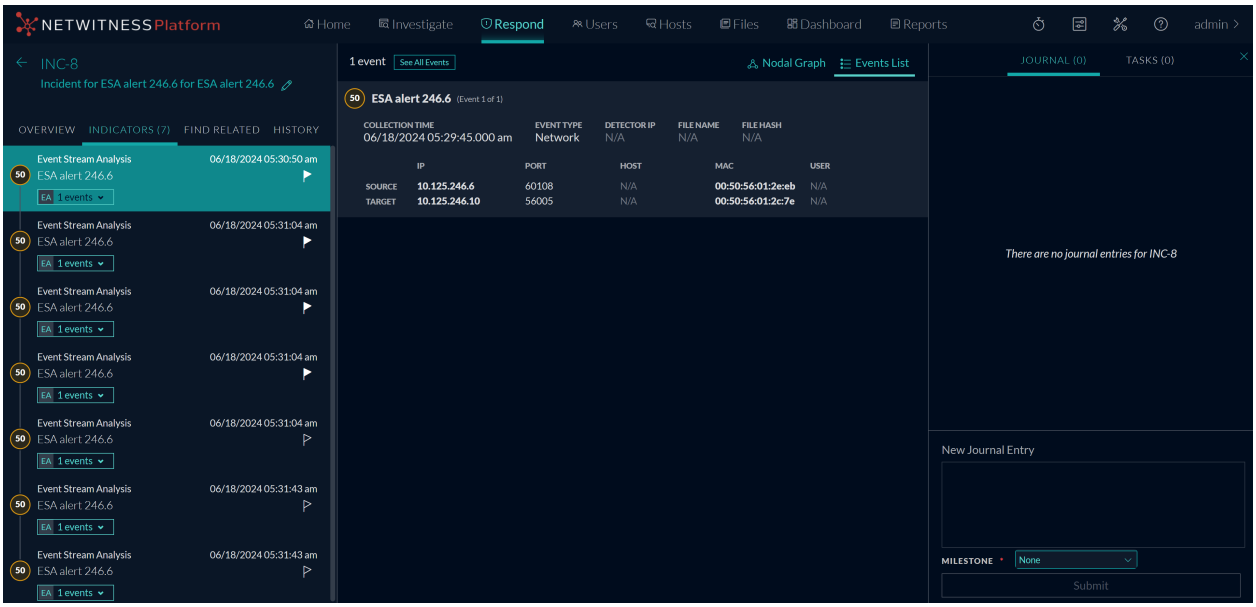


Persist and Suspend Persist Events

Persist an event to retain the event and thereby, copy the event data from the regular database into a long-term storage cache within the NetWitness source. Suspend persist the event to delete the event in the long-term storage cache.

- To persist an event, click the flag listed under each of the event. The selected flag is highlighted, and the message Event Persisted successfully appears.
- To suspend persist event, click a highlighted flag (persisted event) once again. The selected flag is no longer highlighted, and the message Suspended Event Persist successfully appears.
- To persist all events in an alert, click the flag at the alert level. The selected flag is highlighted along with all the flags associated with events of the alert.

- To suspend persist all events in an alert, click the flag at the alert level. The selected flag is highlighted along with all the flags associated with events of the alert.



Change Event Retention

Incidents can contain multiple persisted events, for which analysis has been completed. They can be suspended from persisting at a time using this feature.

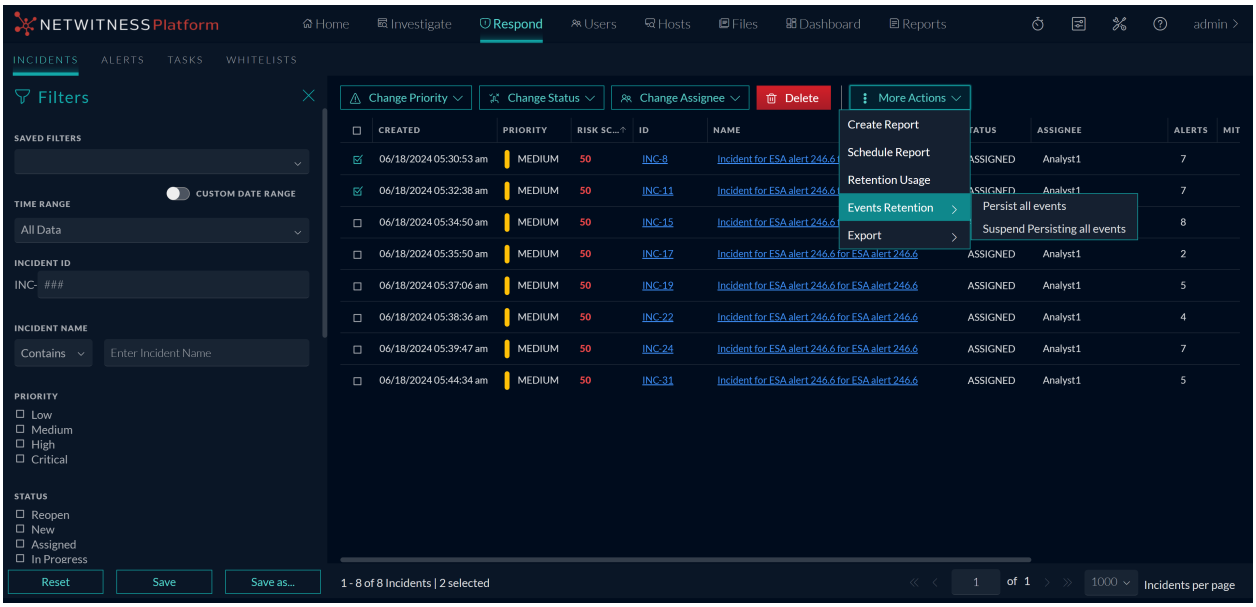
Note: A maximum of 1 incident can be persisted or suspend persisted at a time in the source NetWitness database. If you try to change event retention for more than 1 incidents, an error message will be displayed. This limitation is introduced to optimize and extract the best performance for this feature. This limit cannot be changed.

To change event retention:

1. Go to **Respond** > **INCIDENTS**.
   All the incidents are listed in the **INCIDENTS** page.
2. Click the selection check-box to select the incident.
3. Click **Change Events Retention** > **Persist all events** or **Suspend Persist all events**.
   The **Confirm change in Retention** window appears.
4. Click **OK**.
   The events in the selected incident are either persisted or suspended from persisting.

Note: You cannot change the event retention for incidents that are in **New** or **Closed** state.

Note: Suspending persist of events in an incident from NetWitness will delete it from the long term cache of the source only. This may not be reversible if the original event data has rolled out in the source database. The events will be deleted permanently.



When you delete incidents or alerts, or suspend persist all the events in an incident, the action will always be successful. However, there are chances for the back-end function to fail due to, but not limited to the following reasons:

- Decoder/Concentrator outage
- Network disruption
- Service Outage

A data retention job is scheduled to run on a daily basis to clean up the events that failed from being deleted. To access the data retention job settings, see To change event retention:

The following table provides information on the parameters that are configured to run the job, which are enabled by default:

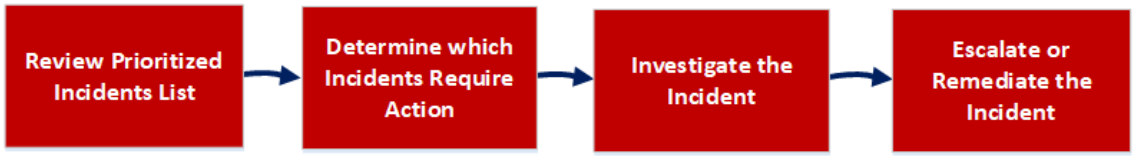
Parameter	Default Setting
`failure-count`	5
`persisted-events-retention-job-enabled`	true - default false.
`persisted-alerts-retention-period`	90 Days

Everyday at a preset time, the data retention job is executed. The default `failure-count` is set to 5 days. If the data retention job is unable to suspend persist an event from the back-end after 5 days, it deletes the event from the repository.

Note: The retention period of risk score context is the same as the retention period of alerts. For example, if the retention period for alerts is set to 90 days, then the retention period of risk score context is also set to 90 days automatically.

Responding to Incidents Workflow

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



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:

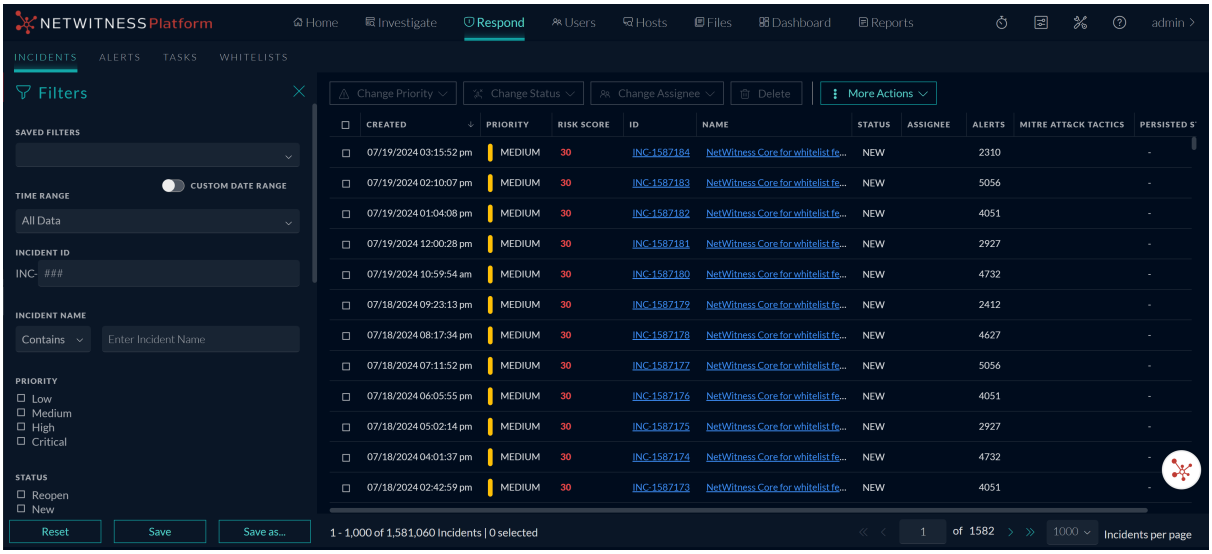
- View the Incidents List
- Filter the Incident List
- Remove My Filters from the Incidents List View
- Save the Current Incidents Filter
- Update a Saved Incidents Filter
- Delete a Saved Incidents Filter
- View My Incidents
- Find an Incident
- Sort the Incidents List
- View Unassigned Incidents

- Assign Incidents to Myself
- Unassign an Incident

View the Incidents List

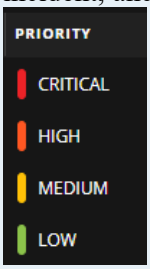
After logging in to NetWitness, most Incident Responders see the Respond view, which is set as the default view. If you have a different initial view, you can navigate to the Respond view.

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

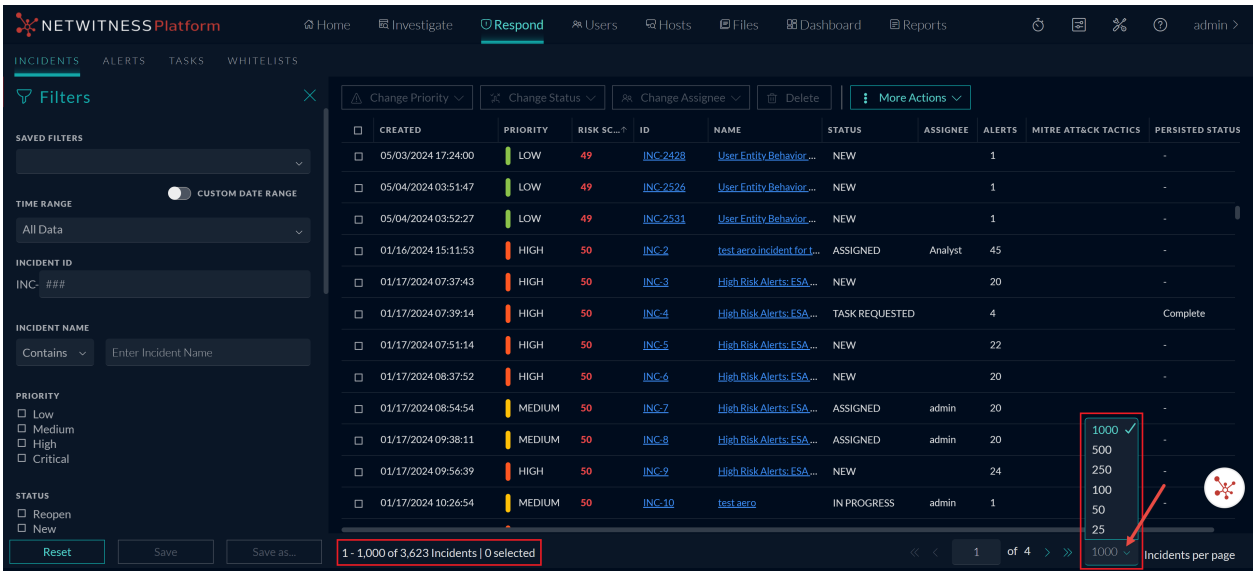


2. If you do not see the incidents list in the Respond view, go to **Respond > Incidents**.
3. Scroll through the incidents list, which shows basic information about each incident as described in the following table.

Column	Description
Created	Shows the creation date of the incident.

Column	Description
Priority	Shows the incident priority. Priority can be Critical, High, Medium, or Low. The Priority is color coded, where red indicates a **Critical** incident, orange represents a **High** risk incident, yellow indicates a **Medium** risk incident, and green represents a **Low** risk incident. For example: 
Risk Score	Shows the incident risk score. The risk score indicates the risk of the incident as calculated using 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: **Reopen**, **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.
MITRE ATT&CK Tactics	Shows the particular Tactic associated with each Incident. For example: **Credential Access**. For more information on MITRE ATT&CK Tactics, see Use MITRE ATT&CK® Framework topic.

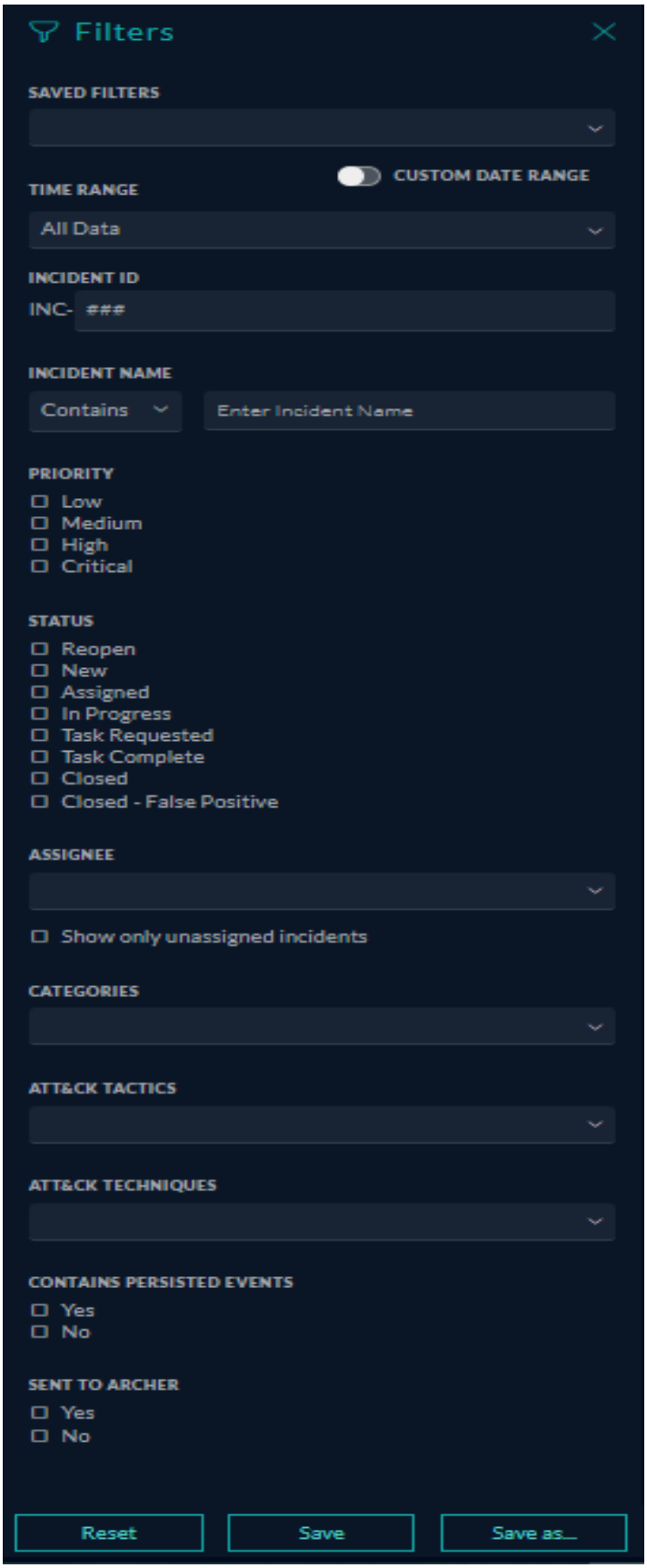
At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number selected. For example: **1 - 500 of 2400 Incidents | 0 selected**. The maximum number of incidents that you can view at one time is 1,000. You can also change the maximum number of incidents per page by selecting from the drop-down at the bottom right corner.



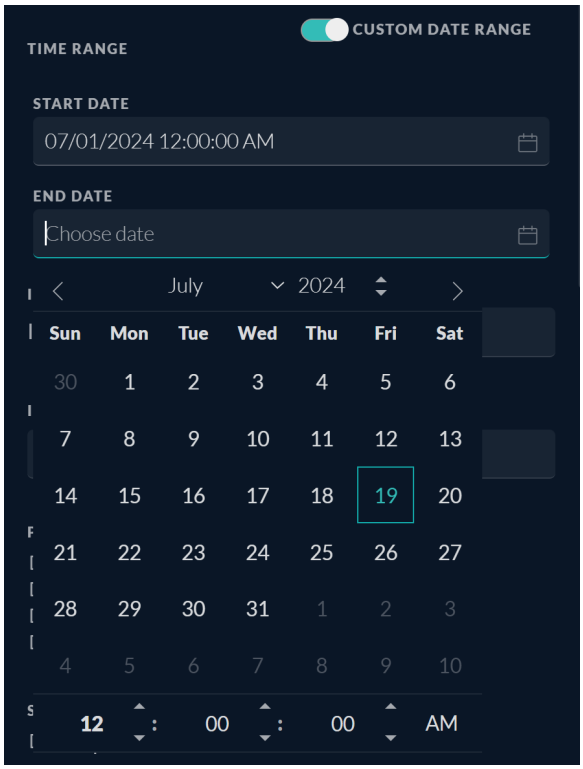
Filter the Incident List

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
SAVED FILTERS
CUSTOM DATE RANGE
TIME RANGE
All Data
INCIDENT ID
INC-
###
INCIDENT NAME
Contains
Enter Incident Name
PRIORITY
Low
Medium
High
Critical
STATUS
Reopen
New
Assigned
In Progress
Task Requested
Task Complete
Closed
Closed - False Positive
ASSIGNEE
Show only unassigned incidents
CATEGORIES
ATT&CK TACTICS
ATT&CK TECHNIQUES
CONTAINS PERSISTED EVENTS
Yes
No
SENT TO ARCHER
Yes
No
Reset
Save
Save as...

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 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.



   - **Incident ID**: Type the number of the incident that you would like to locate. For example, for INC-1050, type only the number "1050" to view the incident.
   - **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.
- **MITRE ATT&CK Tactics**: Select the tactic associated with the incident.
- **MITRE ATT&CK Techniques**: Select the technique associated with the incident.
- **Sent to Archer**: (In version 11.2 and later, if 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**.
- **CONTAINS PERSISTED EVENTS**: Select a filter to view incidents based on the persisted events.

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.

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

Remove My Filters from the Incidents List View

NetWitness remembers your filter selections in the Incidents 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**.

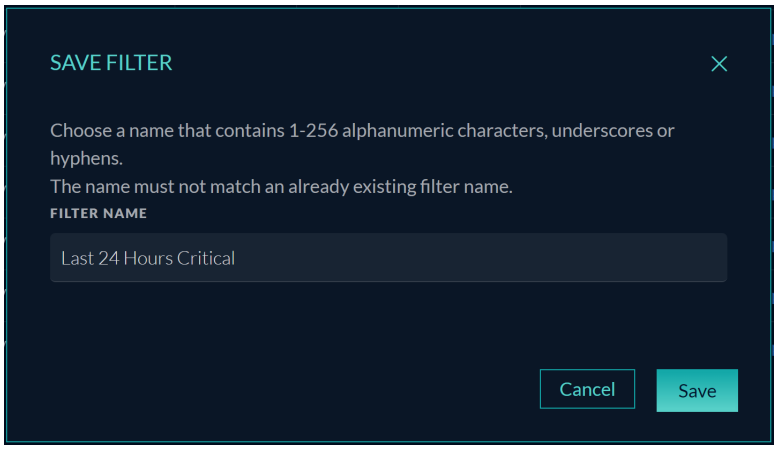
Save the Current Incidents Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

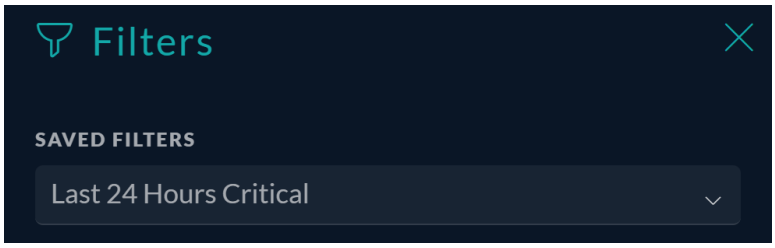
Saved filters provide a way for analysts to save and quickly apply specific filter conditions to the list of incidents. You can also use these filters to customize the Springboard landing page. For example, you may want to create a filter to show only critical incidents over the last 24 hours.

Saved filters are global. You can save a filter for other analysts to use and you can use any saved filter.

1. In the Filters panel, select one or more options to filter the incidents list. For example, in the Time Range field, select Last 24 Hours, and for Priority, select Critical.
2. Click **Save As** and in the **Save Filter** dialog, enter a unique name for the filter and save it, for example Last24Hours-Critical.



The filter is added to the **Saved Filters** list.



Update a Saved Incidents Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

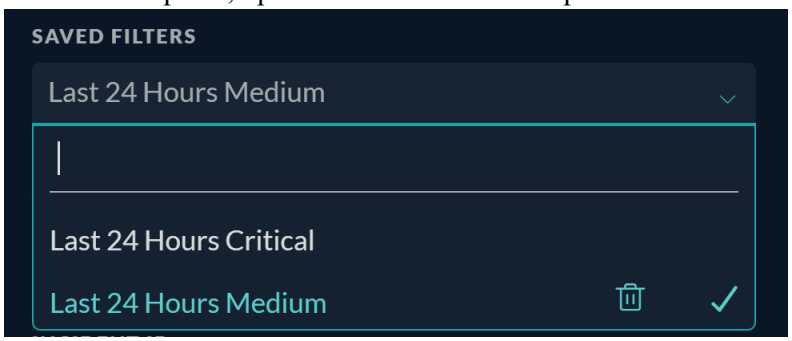
1. In the Filters panel **Saved Filters** drop-down list, select a saved filter.
2. Update your filter selections and click **Save**.

Delete a Saved Incidents Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

When a saved filter is no longer required, you can remove it from the saved filters list. Filters used in the Springboard cannot be deleted.

1. In the Filters panel, open the **Saved Filters** drop-down list.

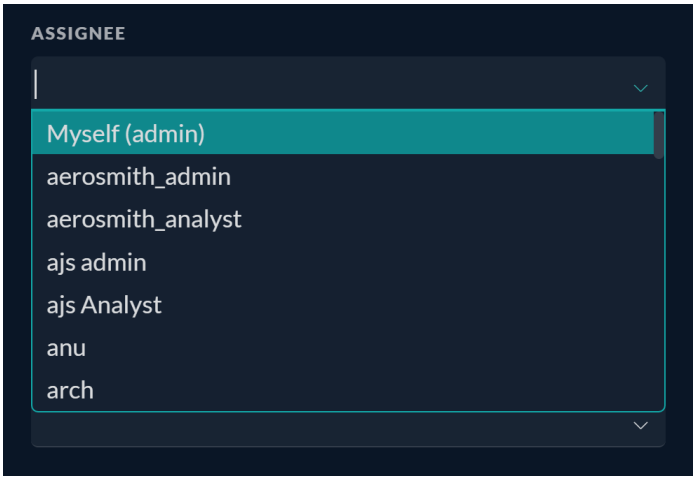


2. Next to the filter name, click  to delete it.

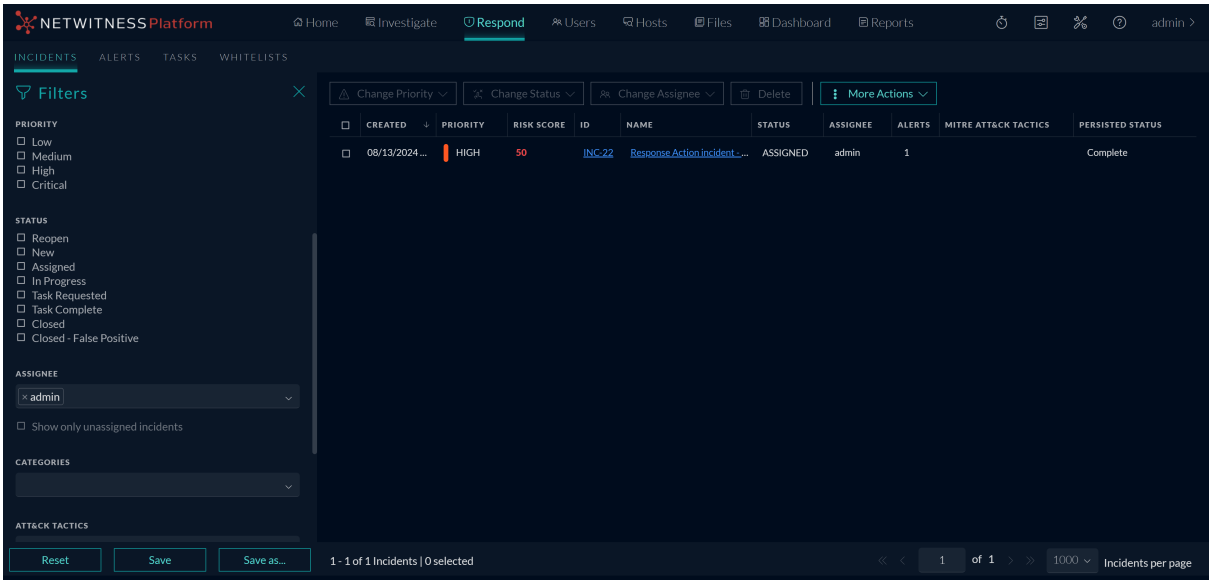
View My Incidents

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

1. If you cannot see the Filter panel, in the Incidents List view toolbar, click  .
2. In the Filter panel, under **Assignee**, select **Myself (your full name)** from the drop-down list.



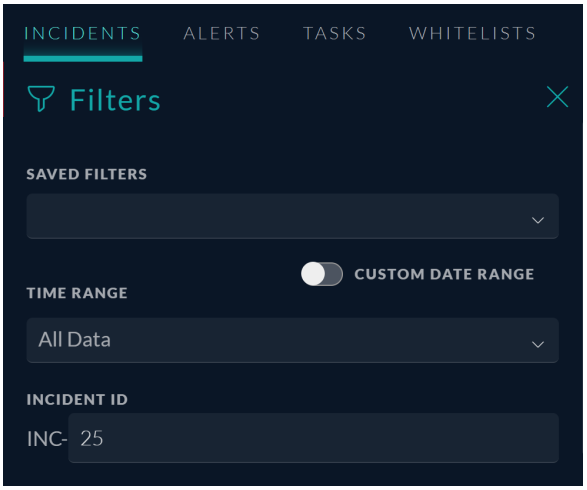
The incidents list shows the incidents that are assigned to you.



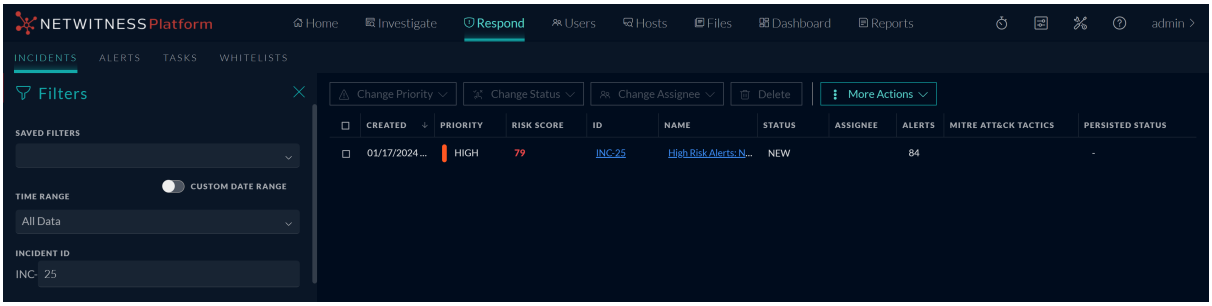
Find an Incident

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 is located 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.

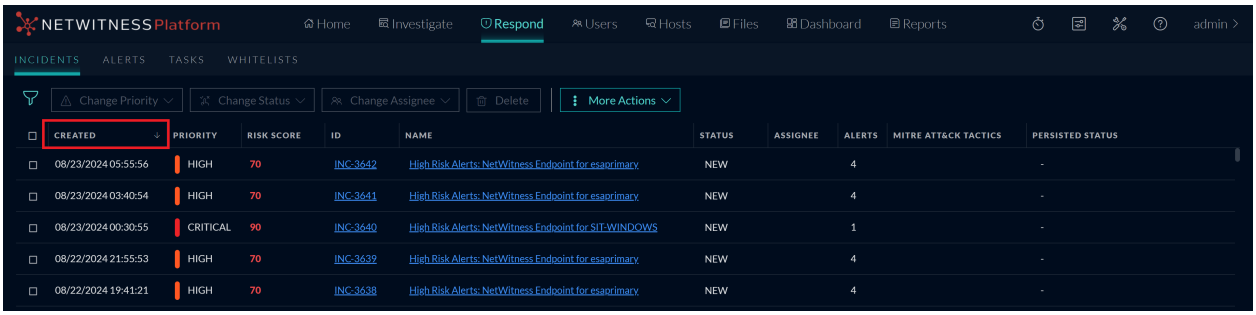


2. In the **INCIDENT ID** field, type the Incident ID for an incident that you would like to locate, for example, type **25** for INC-25.
   The specified incident appears in your incident list. If you do not see any results, try resetting your filters.



Sort the Incidents List

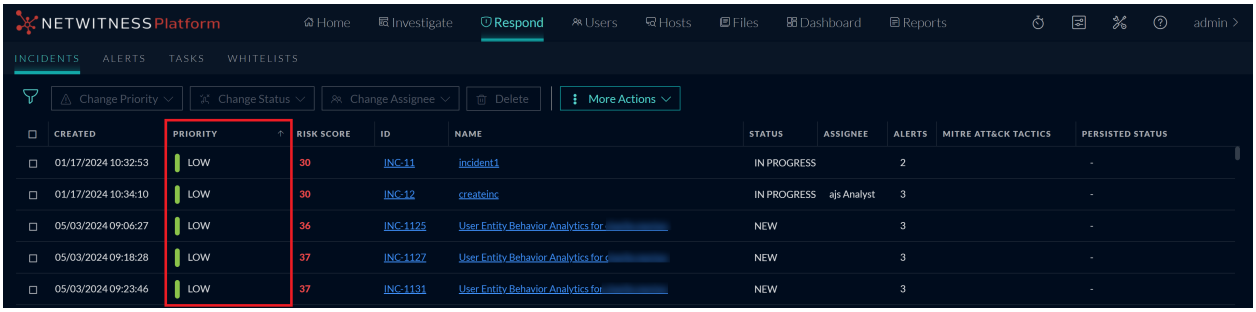
The default sort for the incidents list is by Created date in descending order  (newest on the top).



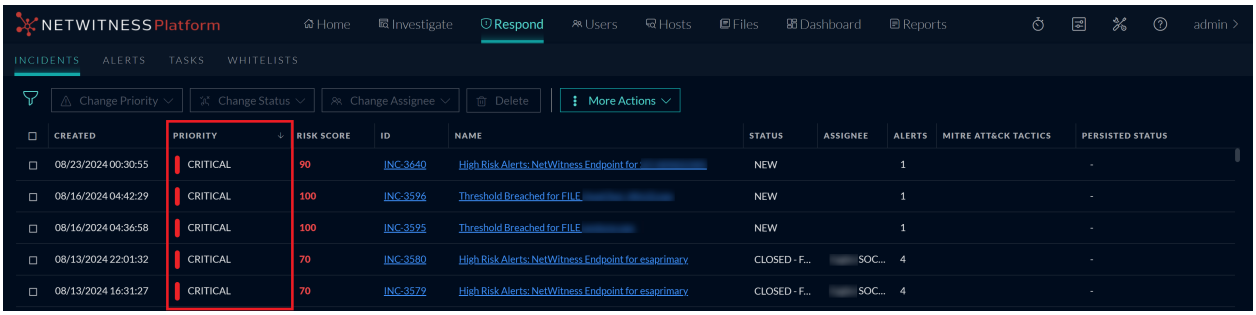
You can change the sort order of the incidents list by clicking a column header in the list.

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).



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.

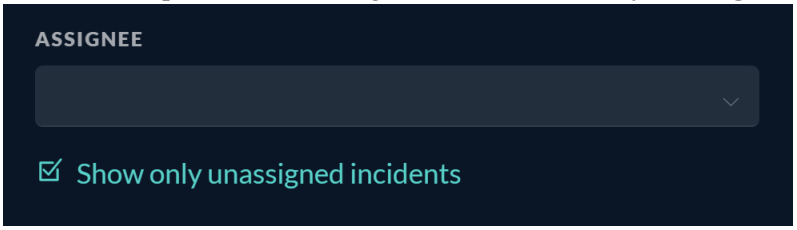


View Unassigned Incidents

Note: This option is available in NetWitness Platform Version 11.1 and later.

You can view unassigned incidents using the Filter.

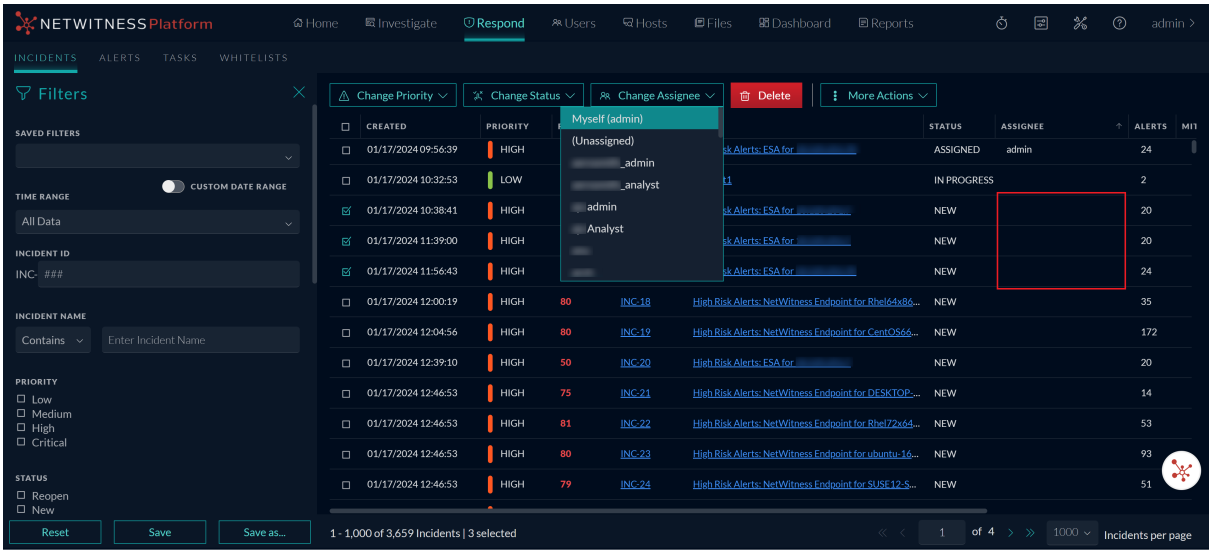
1. If you cannot see the Filter panel, in the Incident List view toolbar, click .
2. In the Filters panel, under Assignee, select **Show only unassigned incidents**.



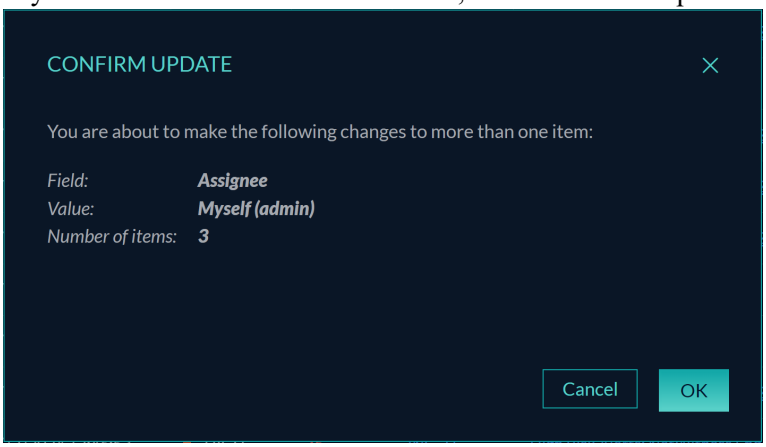
The incidents list is filtered to show unassigned incidents.

Assign Incidents to Myself

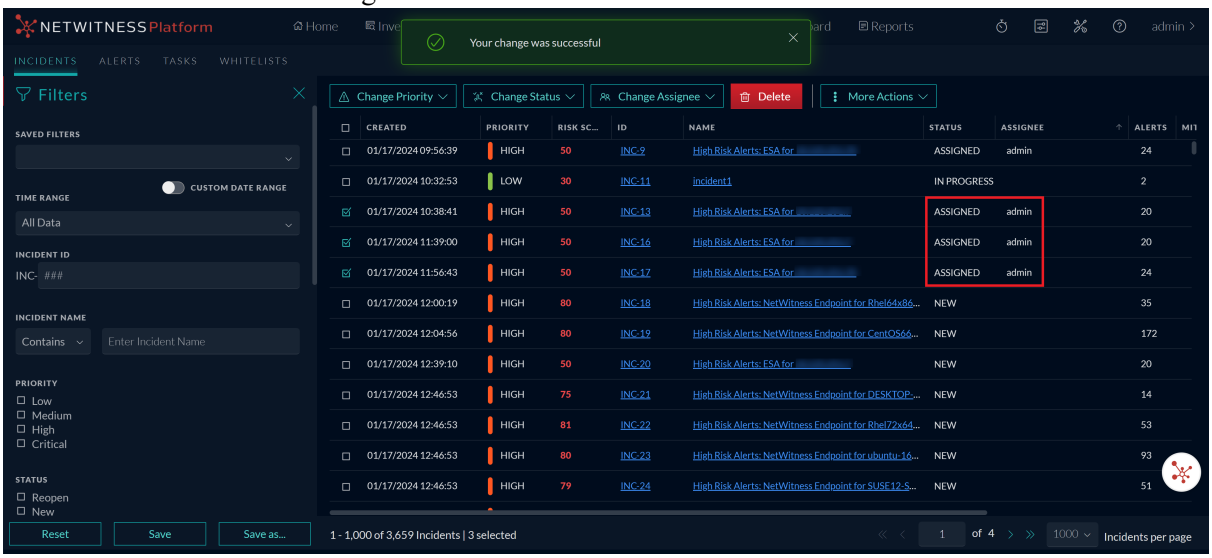
1. In the Incident List view, select one or more incidents that you want to assign to yourself.
2. Click **Change Assignee** and select **Myself (your full name)** from the drop-down list.



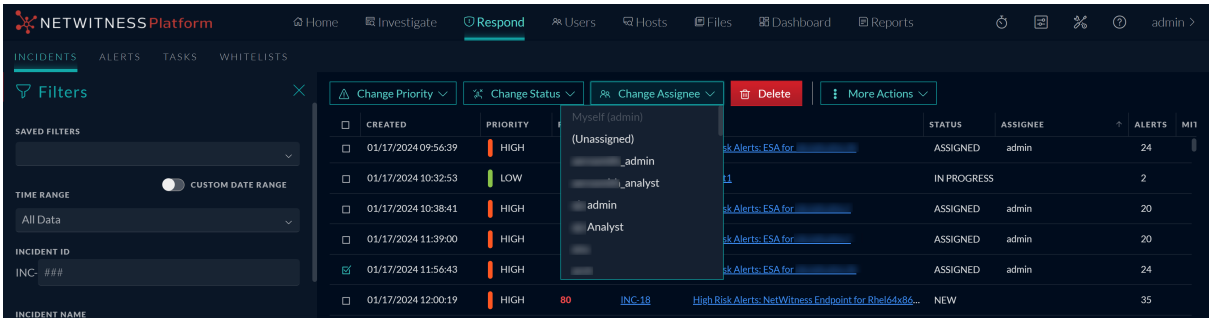
3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.



You can see a successful change notification.

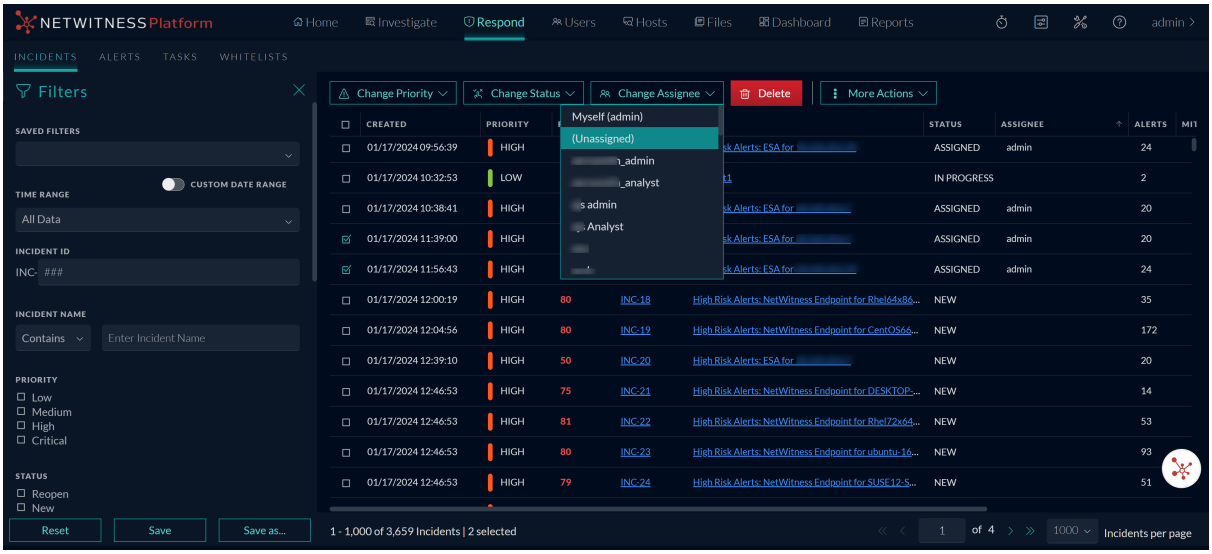


Note: On selecting any particular incident, current assignee name is grayed out under **Change Assignee** drop-down list. This is not applicable in case multiple incidents are selected. Refer the following figure.

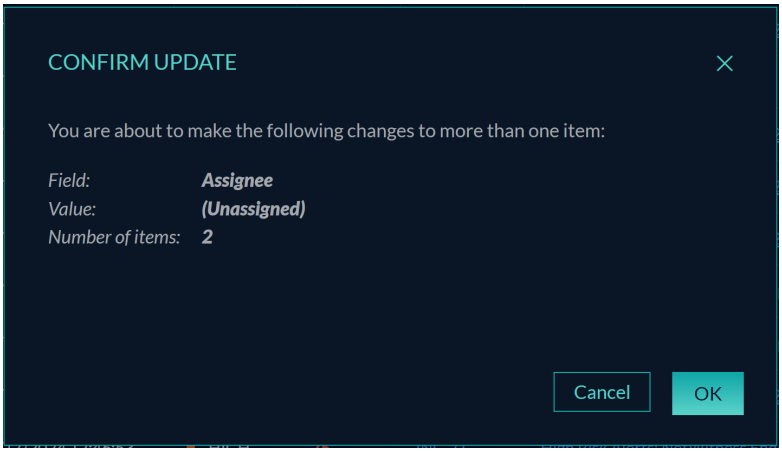


Unassign an Incident

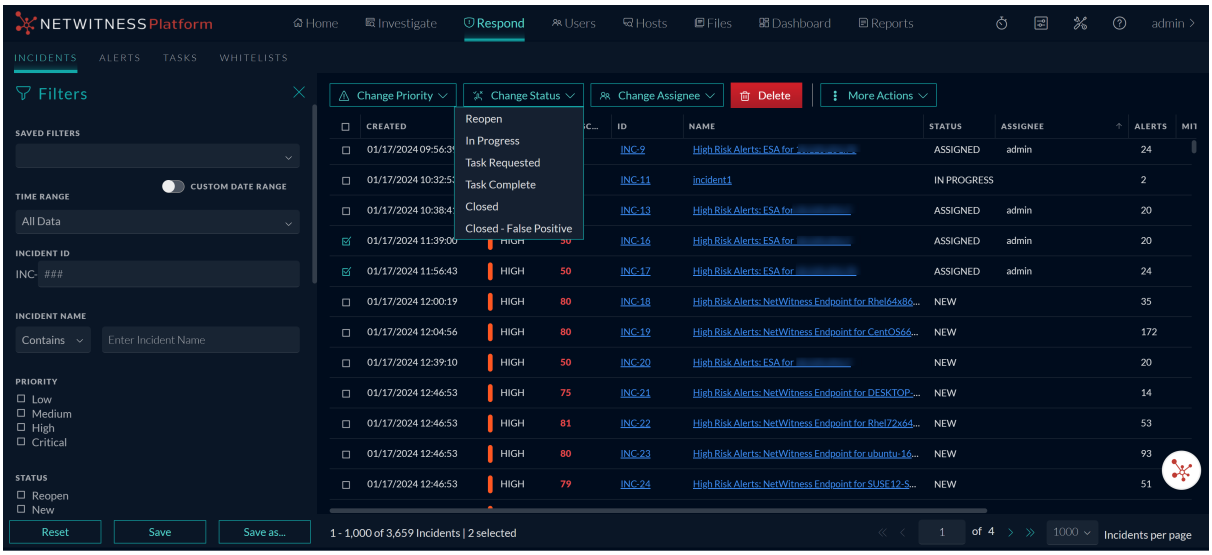
1. In the Incident List view, select one or more incidents that you want to unassign.
2. Click **Change Assignee** and select **(Unassigned)** from the drop-down list.



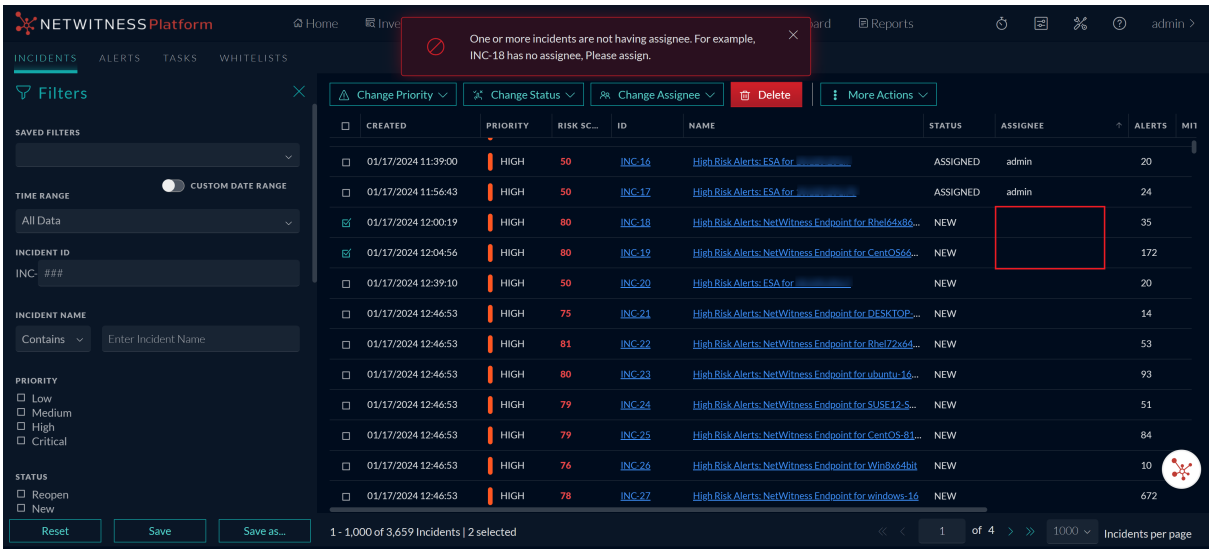
3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.

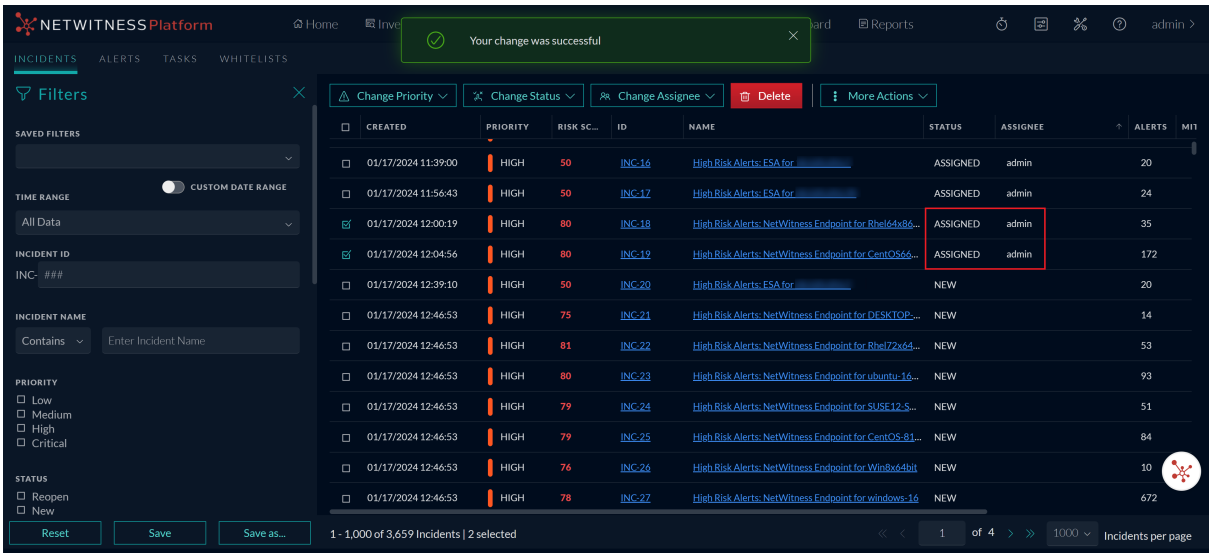


4. Verify that the Status is still correct and make changes as required. To change the status, select one or more incidents, click **Change Status**, and select a new status.



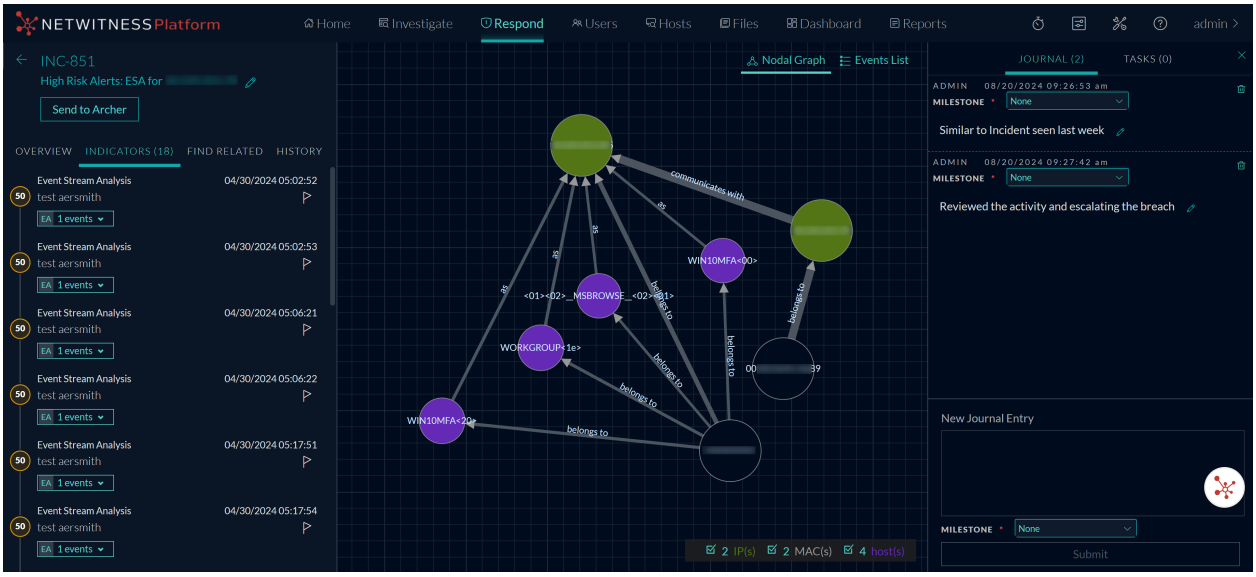
Note: You must assign the incidents to change their status. If you try to change the incident status without assigning the incident, the error message **One or more incidents are not having assignee. For example, INC-x has no assignee, Please assign.** is displayed. Refer the following figures.




NETWITNESS Platform
Home
Reports
admin
Your change was successful
INCIDENTS
ALERTS
TASKS
WHITELISTS
Filters
SAVED FILTERS
CUSTOM DATE RANGE
TIME RANGE
All Data
INCIDENT ID
INC- ###
INCIDENT NAME
Contains
Enter Incident Name
PRIORITY
Low
Medium
High
Critical
STATUS
Reopen
New
Reset
Save
Save as...
Change Priority
Change Status
Change Assignee
Delete
More Actions
CREATED
PRIORITY
RISK SC...
ID
NAME
STATUS
ASSIGNEE
ALERTS
01/17/2024 11:39:00 HIGH 50 INC-16 High Risk Alerts: ESA for ASSIGNED admin 20
01/17/2024 11:56:43 HIGH 50 INC-17 High Risk Alerts: ESA for ASSIGNED admin 24
01/17/2024 12:00:19 HIGH 80 INC-18 High Risk Alerts: NetWitness Endpoint for Rhel64x86... ASSIGNED admin 35
01/17/2024 12:04:56 HIGH 80 INC-19 High Risk Alerts: NetWitness Endpoint for CentOS66... ASSIGNED admin 172
01/17/2024 12:39:10 HIGH 50 INC-20 High Risk Alerts: ESA for NEW 20
01/17/2024 12:46:53 HIGH 75 INC-21 High Risk Alerts: NetWitness Endpoint for DESKTOP-... NEW 14
01/17/2024 12:46:53 HIGH 81 INC-22 High Risk Alerts: NetWitness Endpoint for Rhel72x64... NEW 53
01/17/2024 12:46:53 HIGH 80 INC-23 High Risk Alerts: NetWitness Endpoint for ubuntu-16... NEW 93
01/17/2024 12:46:53 HIGH 79 INC-24 High Risk Alerts: NetWitness Endpoint for SUSE12-S... NEW 51
01/17/2024 12:46:53 HIGH 79 INC-25 High Risk Alerts: NetWitness Endpoint for CentOS-81... NEW 84
01/17/2024 12:46:53 HIGH 76 INC-26 High Risk Alerts: NetWitness Endpoint for Win8x64bit NEW 10
01/17/2024 12:46:53 HIGH 78 INC-27 High Risk Alerts: NetWitness Endpoint for windows-16 NEW 672
1 - 1,000 of 3,659 Incidents | 2 selected
1
of 4
1000
Incidents per page

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.

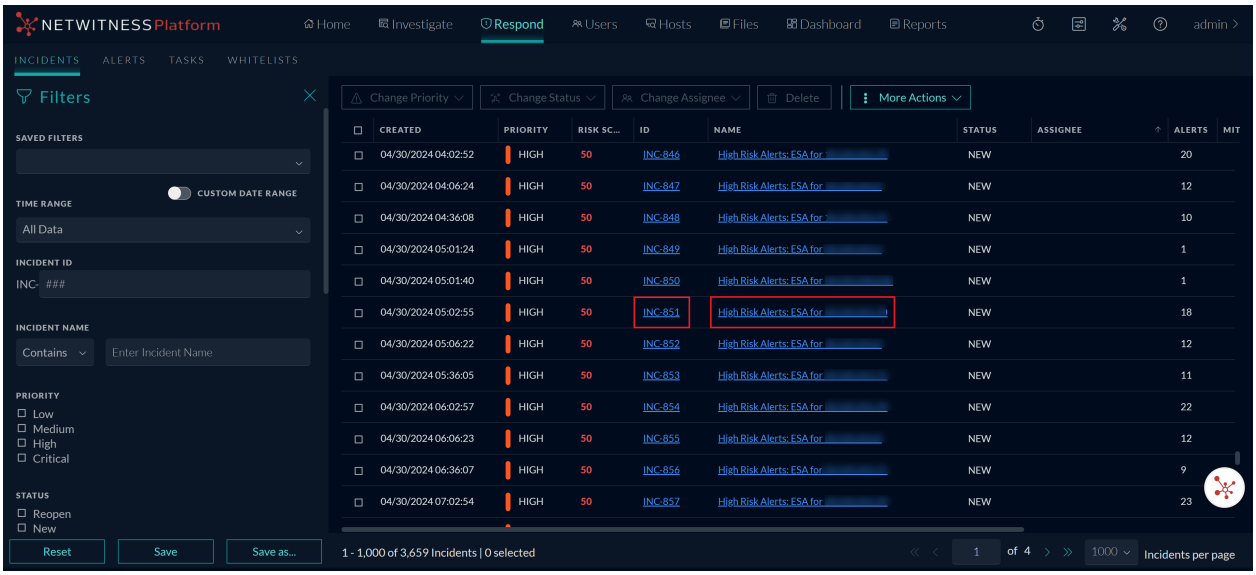


You can perform the following procedures in the Incident Details view to determine the action required on an incident:

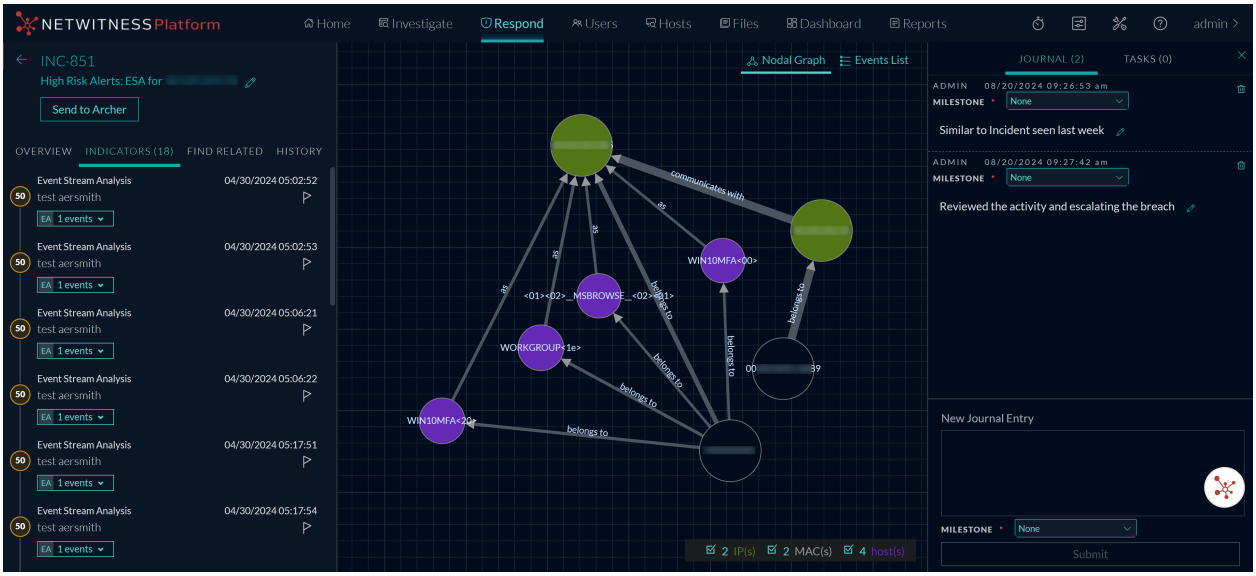
- View Incident Details
- View Basic Summary Information about the Incident
- View the Indicators and Enrichments
- View and Study the Events
- View C2 Enrichment Information for Suspected C&C Incidents
- View and Study the Entities Involved in the Events on the Nodal Graph
- Nodal Graph Behaviors and Characteristics
- 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.



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

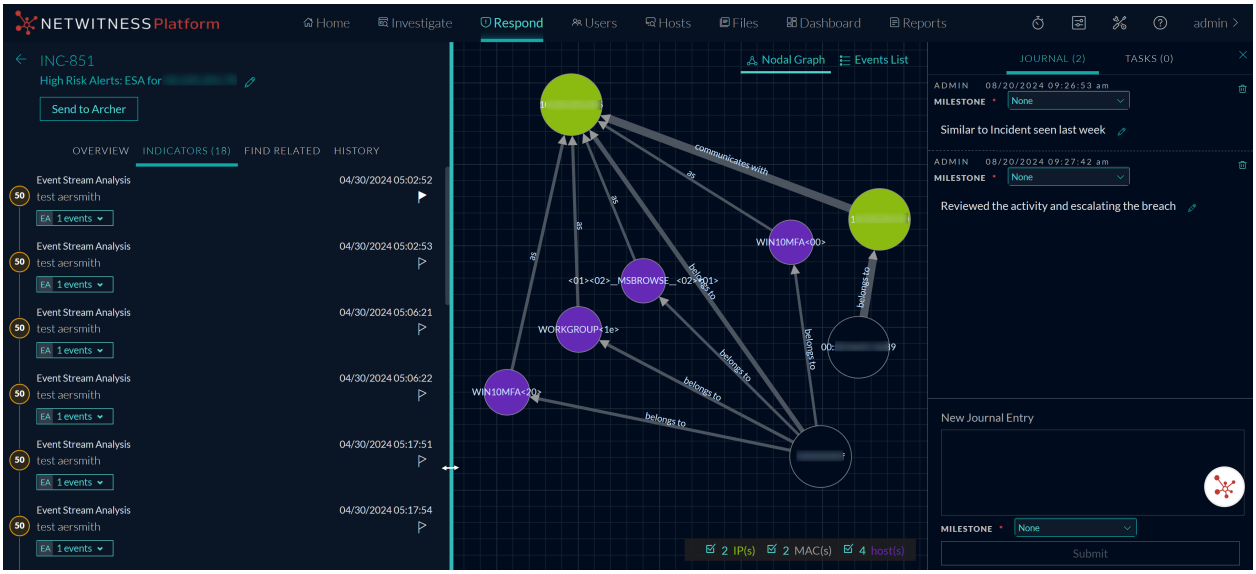


The Incident Details view has the following panels:

- **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 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.
- **Related Indicators**: The Related Indicators panel enables you to search the NetWitness alerts database to find alerts that are related to this incident. You can also add related alerts that you find to the incident.
- **History**: The History panel allows you to view the different actions performed by the user on an incident. Events such as Incident Assignee change, Incident Status change, Incident Priority change, and Incident creation are recorded in this panel.
- **Nodal Graph**: The nodal graph is an interactive graph that shows the relationship between the entities involved in the incident. An *Entity* is represented by an 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.

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:

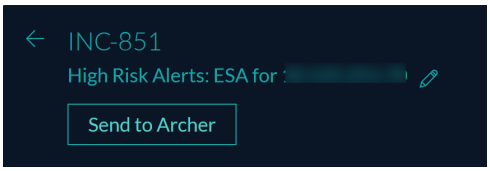


View Basic Summary Information about the Incident

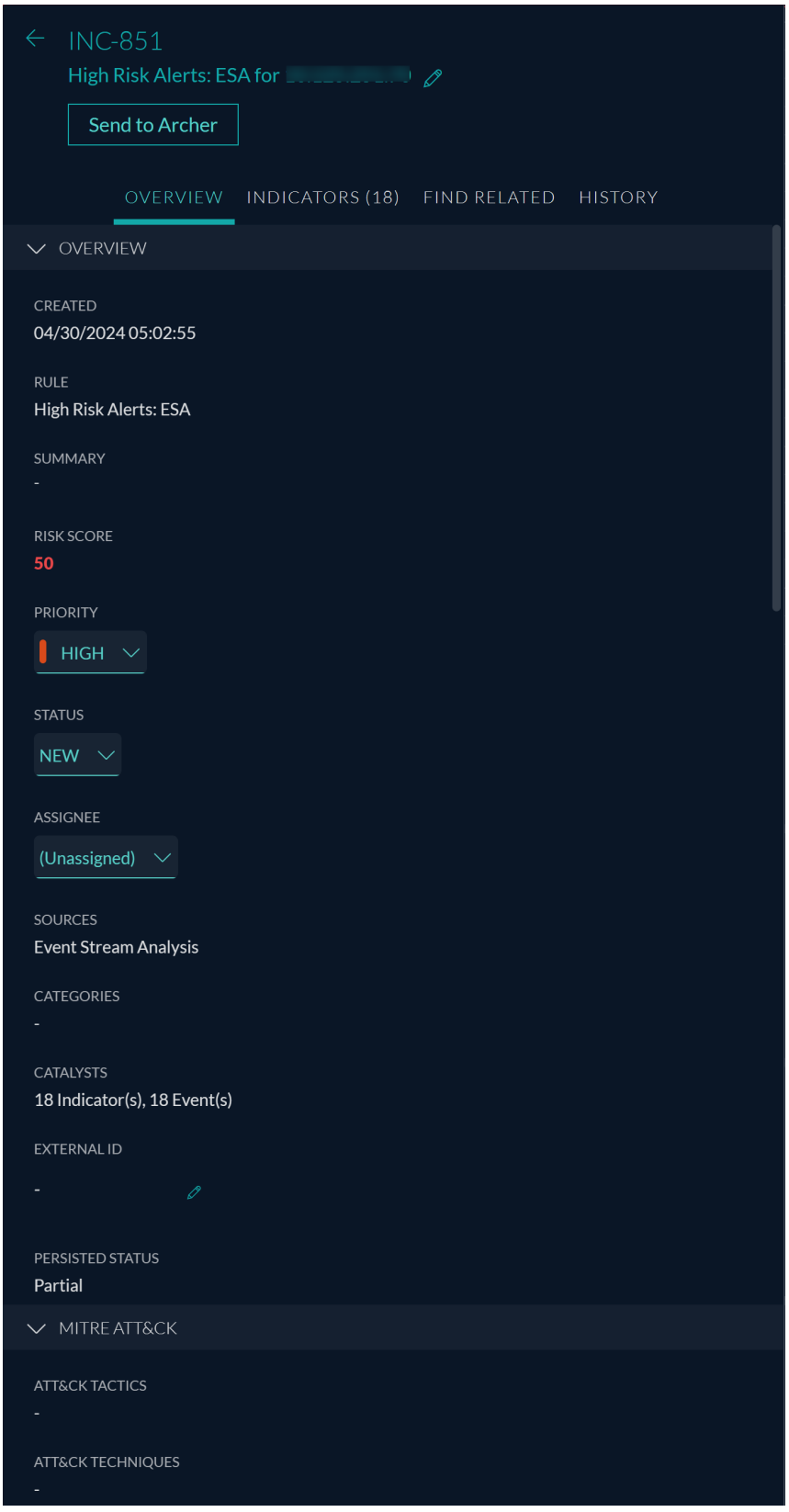
You can view basic summary information about an incident in the Overview panel.

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

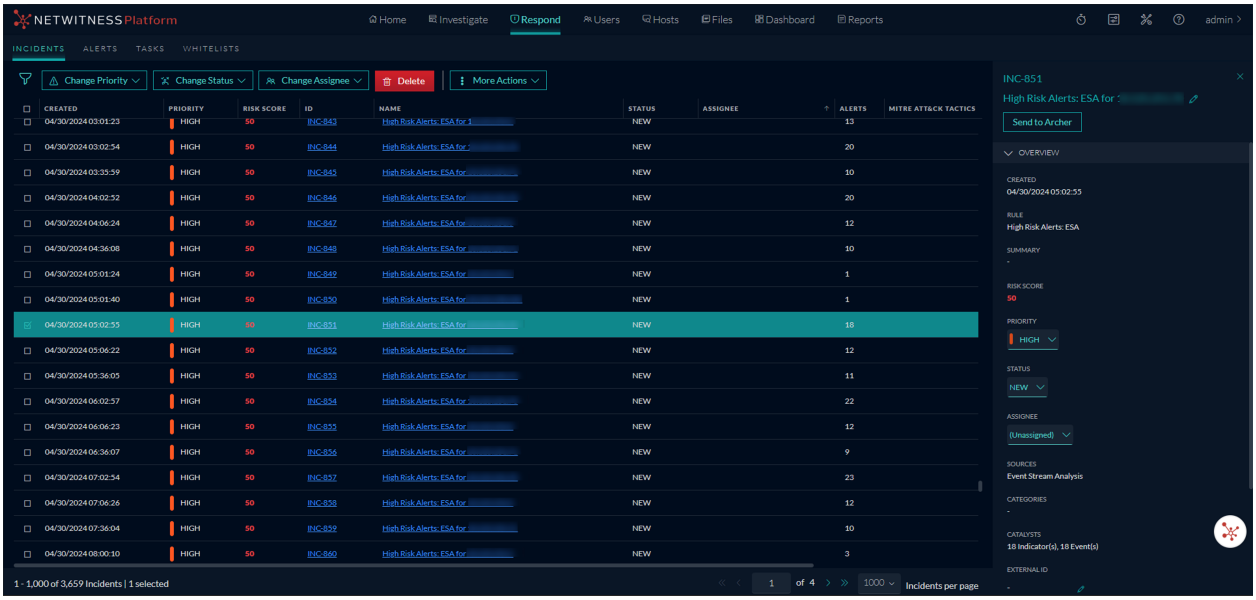
- **Incident ID**: This is an automatically created unique ID assigned to the incident.
- **Name**: The incident name is derived from the rule used to trigger the incident.
- **Send to Archer / Sent to Archer**: (In version 11.2 and later, if Archer is configured as a data source in Context Hub, you 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.


INC-851
High Risk Alerts: ESA for
Send to Archer
OVERVIEW
INDICATORS (18)
FIND RELATED
HISTORY
OVERVIEW
CREATED
04/30/2024 05:02:55
RULE
High Risk Alerts: ESA
SUMMARY
-
RISK SCORE
50
PRIORITY
HIGH
STATUS
NEW
ASSIGNEE
(Unassigned)
SOURCES
Event Stream Analysis
CATEGORIES
-
CATALYSTS
18 Indicator(s), 18 Event(s)
EXTERNAL ID
-
PERSISTED STATUS
Partial
MITRE ATT&CK
ATT&CK TACTICS
-
ATT&CK TECHNIQUES
-

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



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

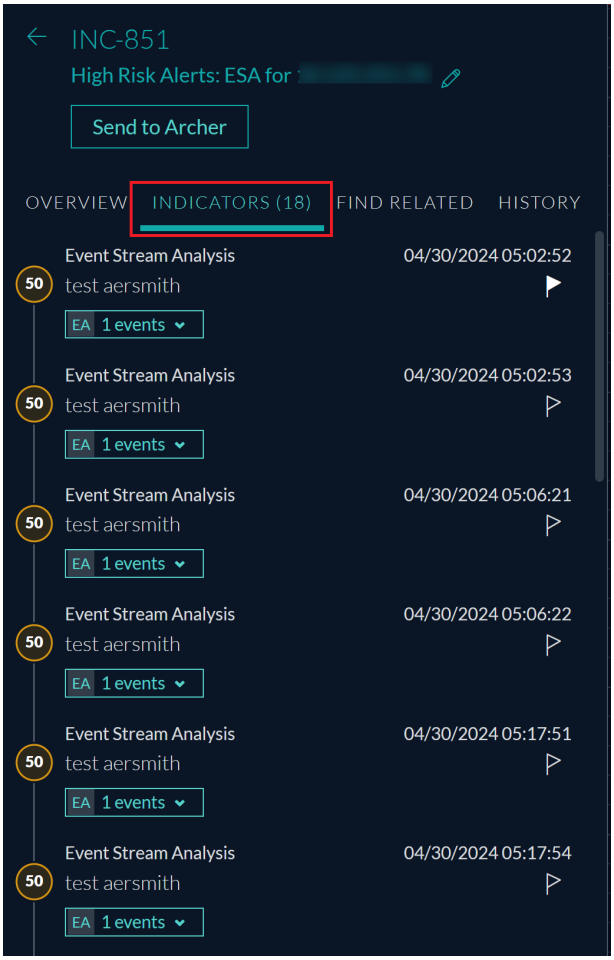
- **Created**: Shows the creation date and time of the incident.
- **Rule / By**: Shows the name of the rule that created the incident or the name of the person who created the incident.
- **Risk Score**: Shows a value between 0 and 100 that indicates the risk of the incident as calculated by an algorithm. 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 Reopen, 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.
- **External ID**: Allows storing the Incident ID referrals from a different platform such as Archer.
- **Time to Acknowledge**: Shows the time taken to assign an Incident after creating it.
- **Time to Detect**: Shows the time taken for completing the task after the Incident is assigned.
- **Time to Resolve**: Shows the time taken for closing the task after the Incident is created.
- **Persisted Status**: Shows the persist status of the Incident. The status can be Complete, Partial, or None (-).

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:

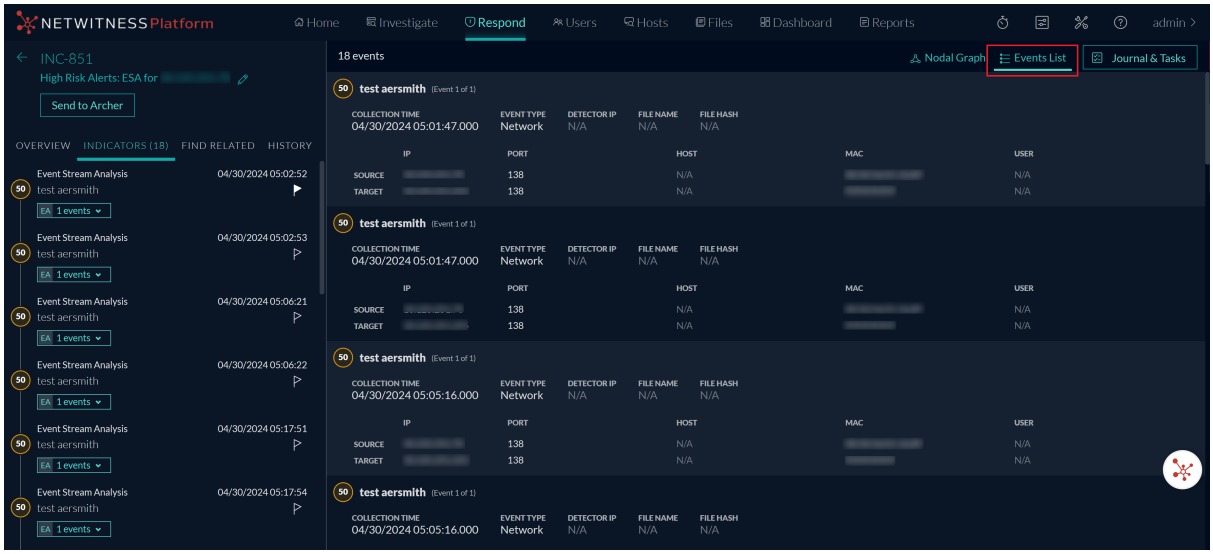
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

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 Events List.



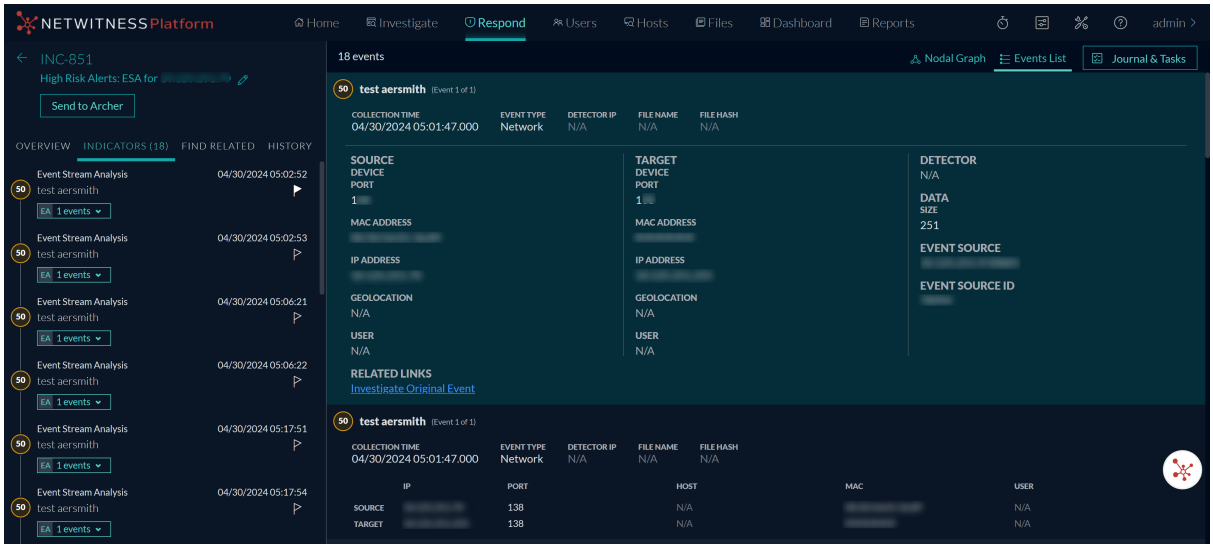
Note: The EVENT TIME displayed on this screen is the same as the COLLECTION TIME from the investigation page.

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.

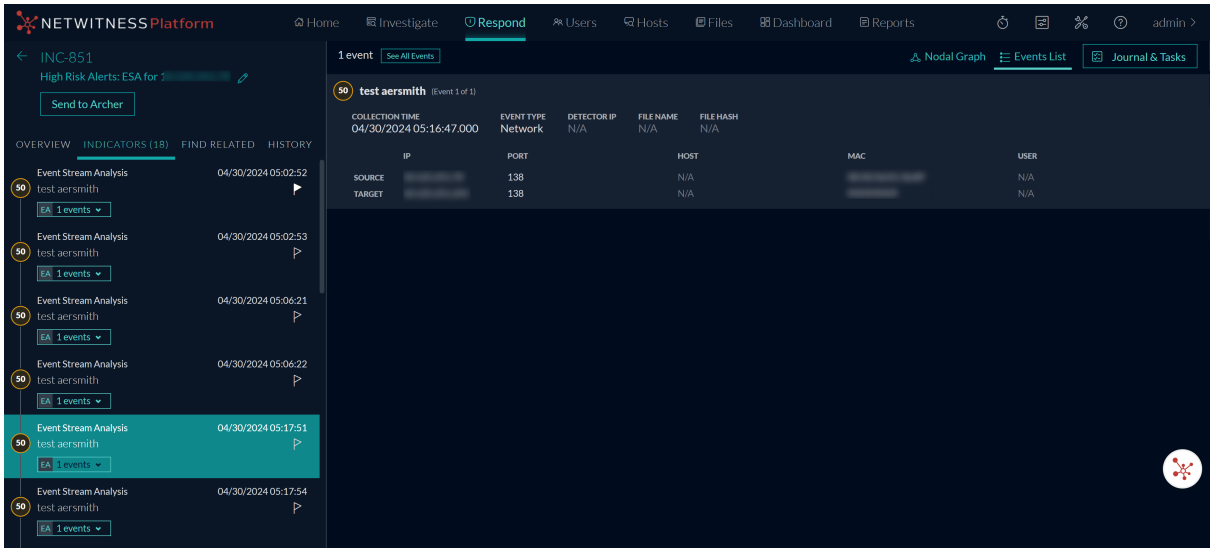
The following table lists typical event information. For details specific to endpoint events, see Events List.

Field	Description
COLLECTION 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.

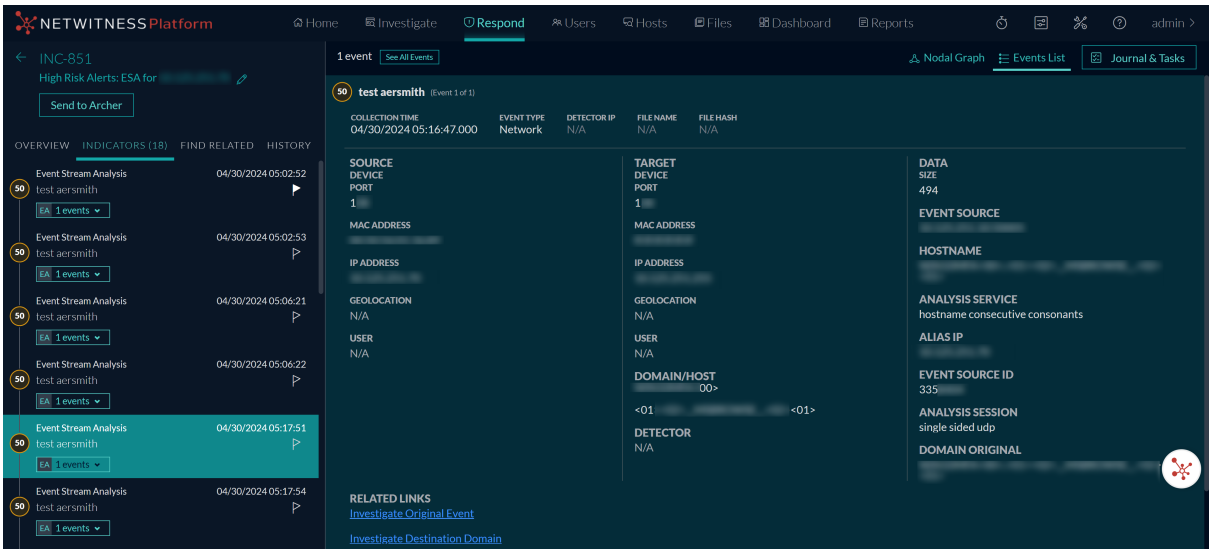
2. Click the top of an event in the Events List to view the event details.
   This example shows the event details for a selected event in the list.



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



4. 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.



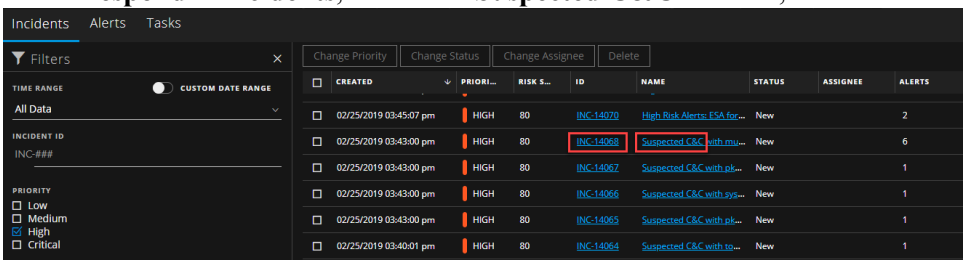
If you have additional Investigate-server permissions, you can also access event analysis details for events. See View Event Analysis Details for Indicators. If you have the UEBA_Analysts role, you can access UEBA details for indicators. See View User Entity Behavior Analytics for Indicators.

View C2 Enrichment Information for Suspected C&C Incidents

Note: This procedure applies only to incidents from ESA Analytics in NetWitness Version 11.3 and 11.4. The Event Stream Analytics Server (ESA Analytics) service, which is used for Automated Threat Detection, is end of life (EOL) and not supported in NetWitness Platform Version 11.5 and later.

The Events List in version 11.3 and later 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.

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

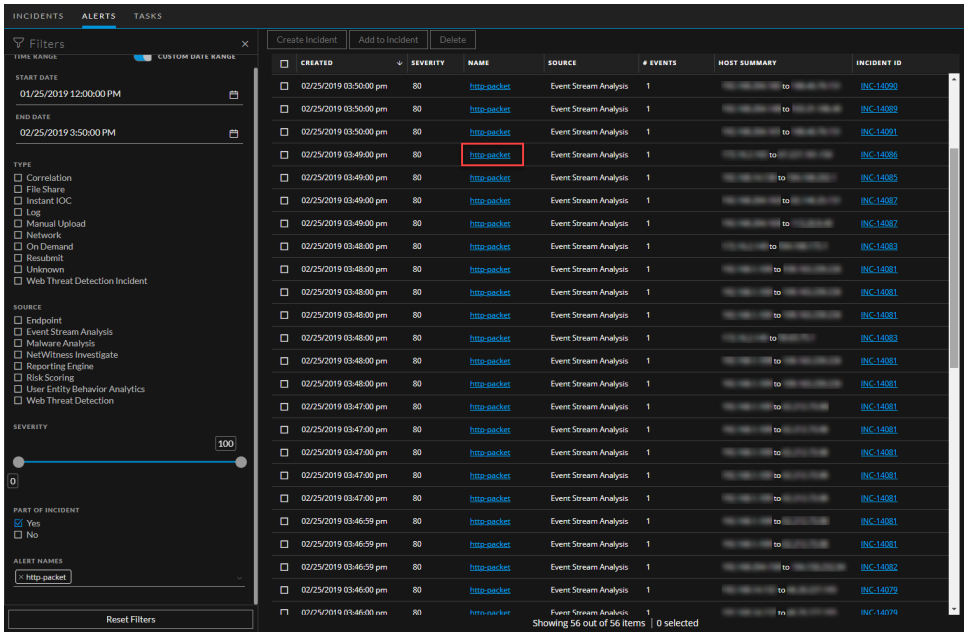


2. Go to **Respond > Alerts** and in the Filters panel, select the following to locate an alert in the Alerts list with the incident ID noted above:

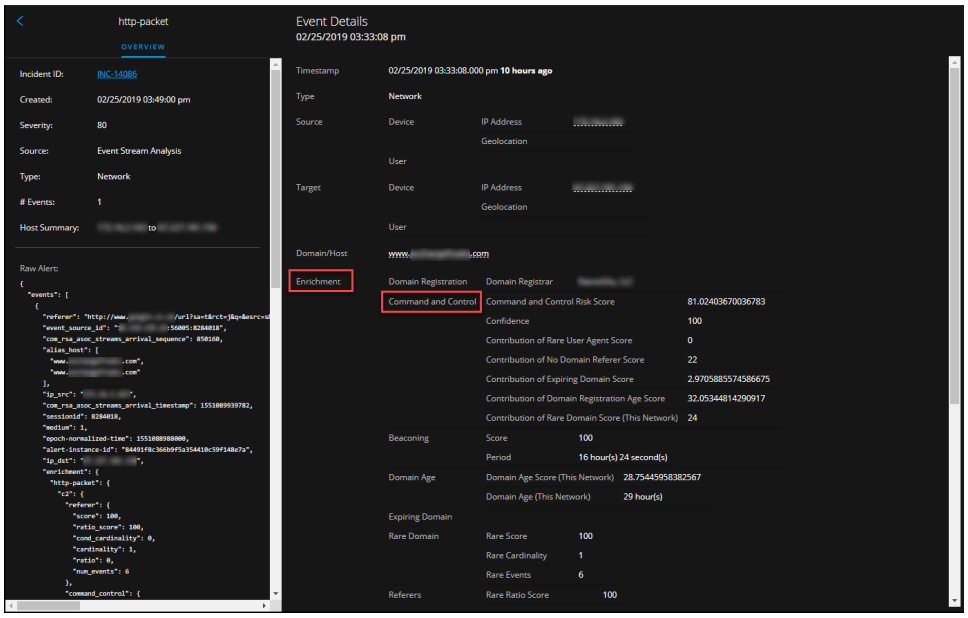
a. In the **Part of Incident** section, select **Yes**.

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.



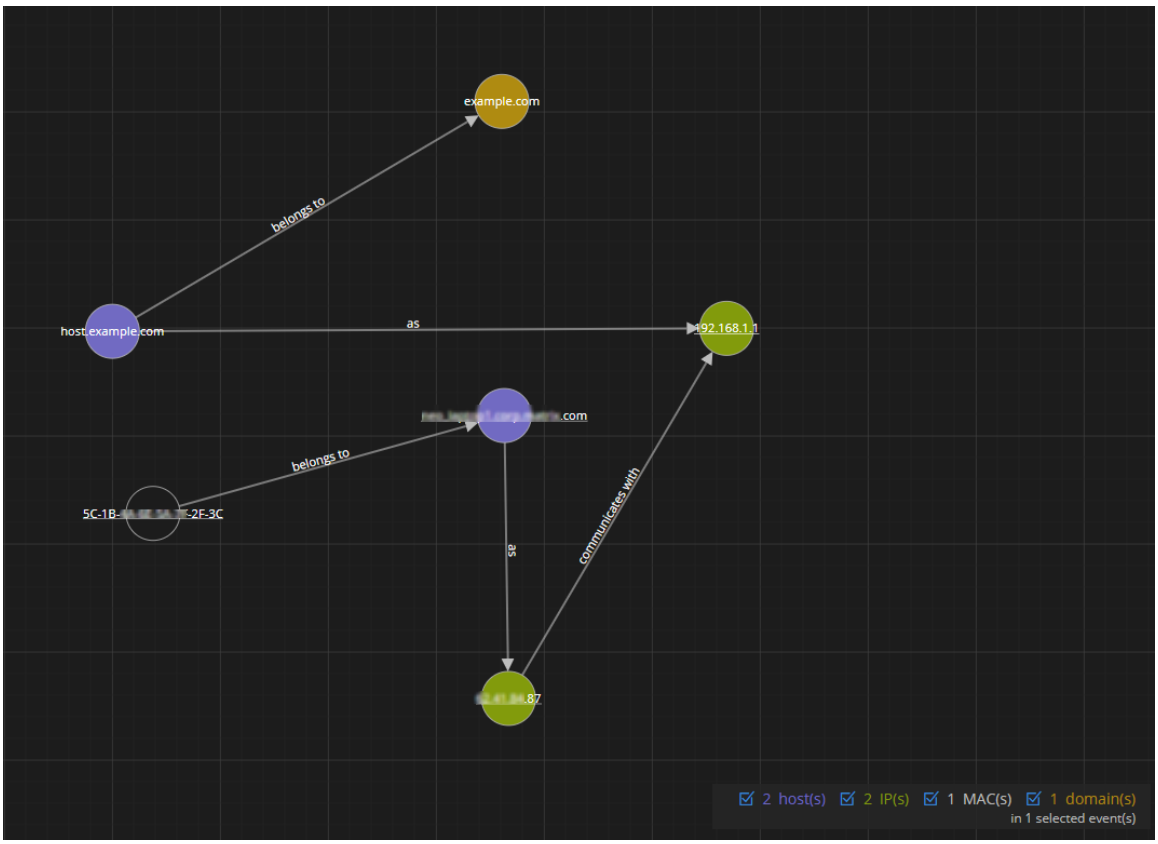
3. In the Alerts list, click the **http-packet** link in the **NAME** field of the alert associated with the incident ID.
The Event Details view shows the C2 enrichment information.



View and Study the Entities Involved in the Events on the Nodal Graph

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 11.3 events, nodes for source filename and file hash are supported, but nodes for target filename and file hash are not supported. In NetWitness 11.4 and later events, nodes for both source and target filenames as well as file hashes are 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.

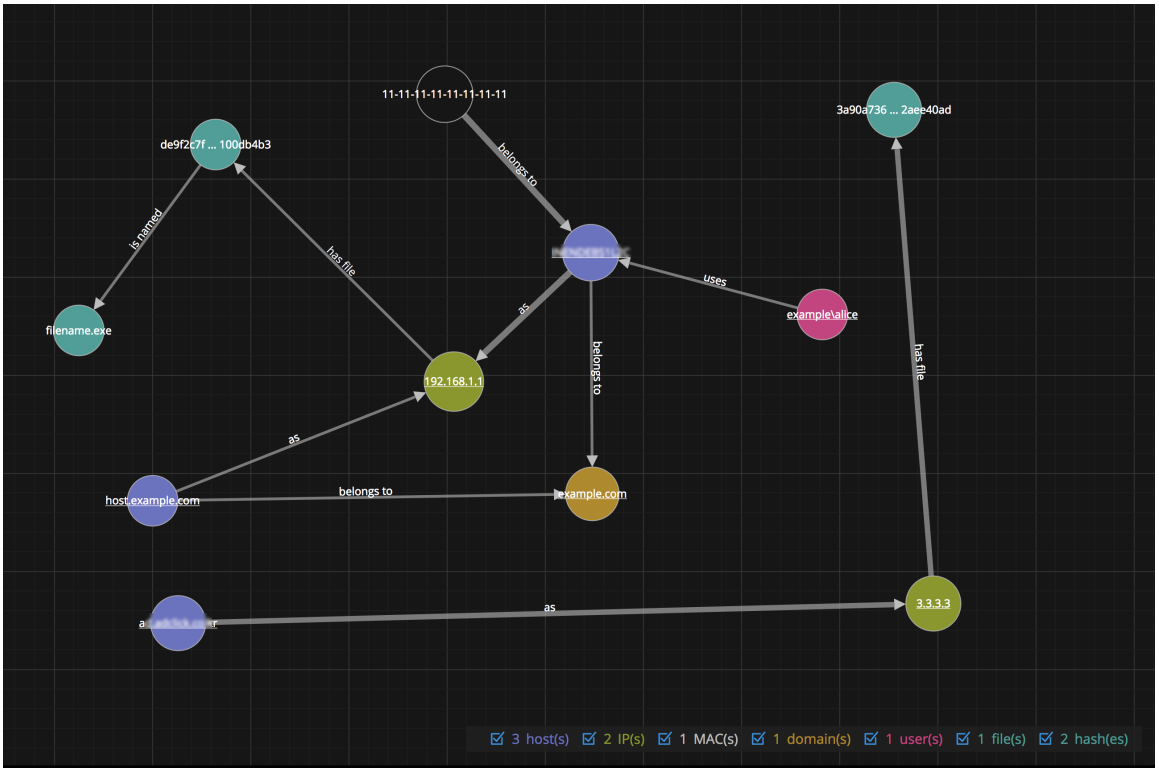
You can click and drag any node to reposition it.

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.
- **Has file**: An arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has file" 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.
- **Calls**: (This arrow is available in NetWitness Platform 11.4 and later.) An arrow between two file hash (checksum) nodes labeled with "calls" indicates the direction of the interaction between the associated files. The source file hash "calls" the target (destination) file hash, which indicates that the source file associated with the source file hash is performing an action on the target file associated with the target file hash.
- **As**: (This relationship type represents attributes of the connected node.) 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.
- **Is named**: (This relationship type represents attributes of the connected node.) 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**: (This relationship type represents attributes of the connected node.) 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.

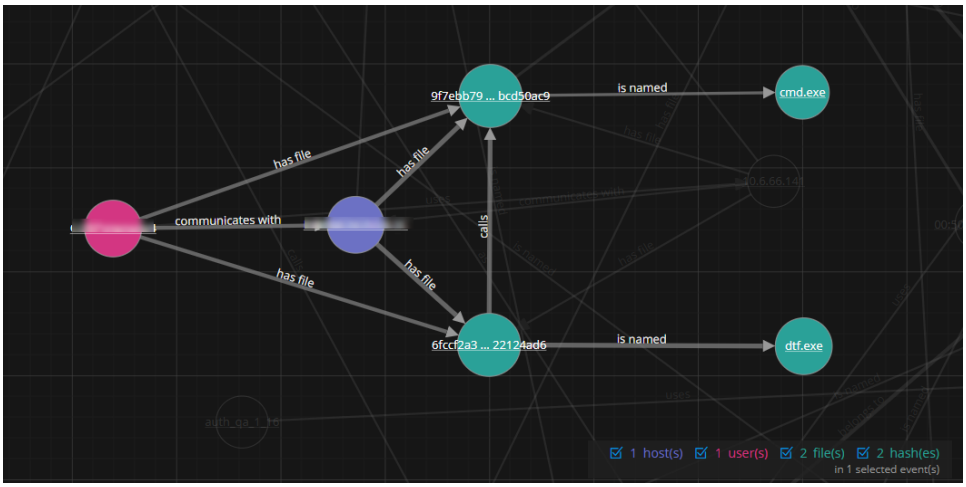
The following nodal graph example has 11 nodes.



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 is one of them) 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.

Note: The following example applies to NetWitness Platform 11.4 and later.

In the following nodal graph example, you can see the interaction between source and target (destination) files. There are six nodes in the selected event.



In this example, the user communicates with a host that has `dtf.eve` and `cmd.exe` files. The `dtf.exe` file on the host "calls" (in this case, launches) the `cmd.exe` file, which is suspected to be malicious activity. Notice that the "calls" arrow appears between the source and target file hashes, which are associated with the files.

Nodal Graph Behaviors and Characteristics

Note: These nodal graph behaviors and characteristics are available in NetWitness Platform Version 11.4 and later.

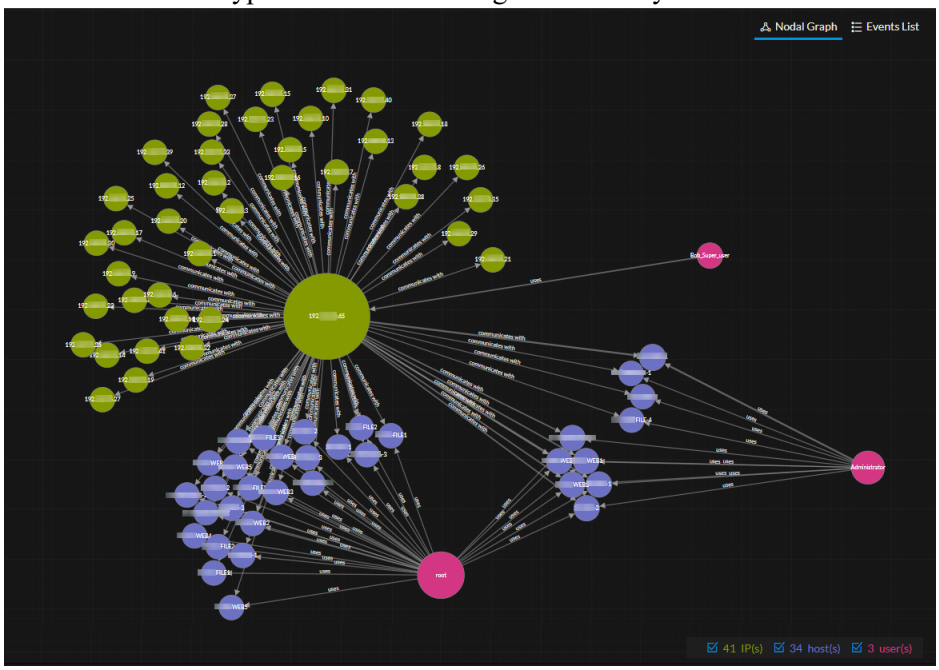
The nodal graph makes it easier for an analyst to get an initial understanding of an incident with minimal effort.

The nodal graph provides the following benefits to an analyst when responding to an incident:

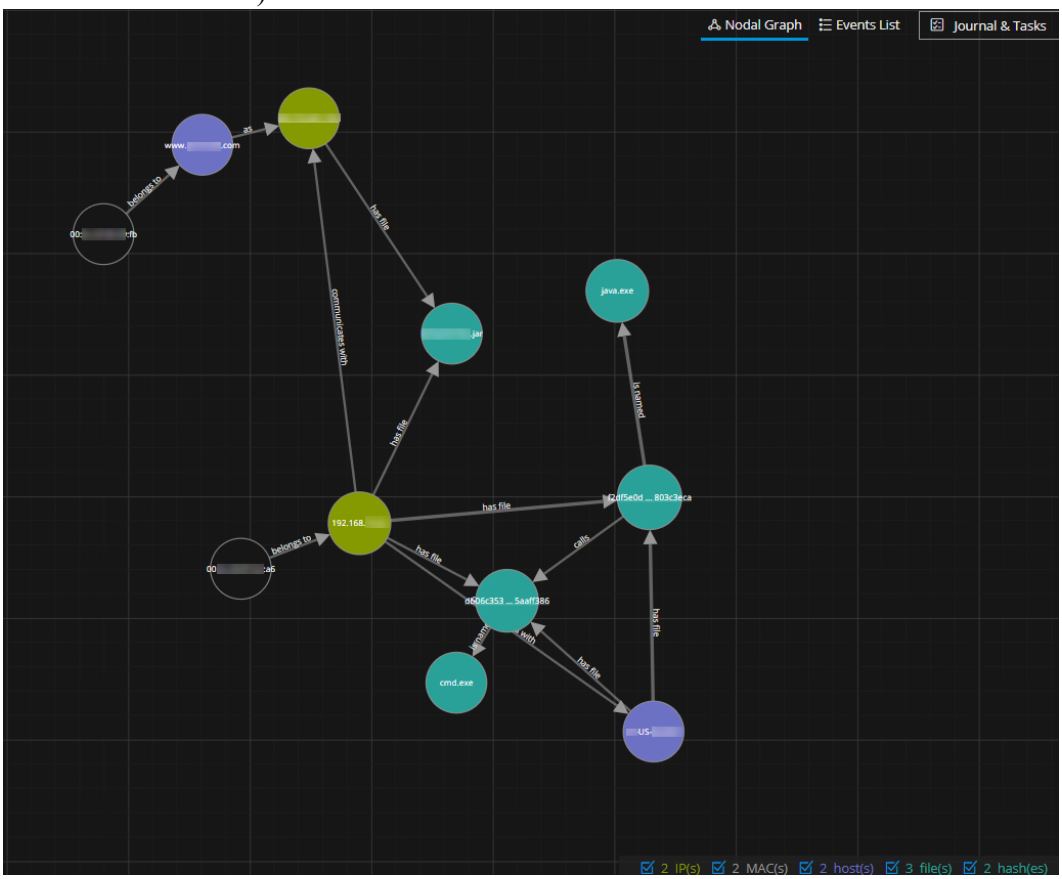
- The nodal graph helps determine scope, commonalities, and outliers in a given dataset, which can be useful context for an analyst.
- In many cases, the initial nodal graph layout presents valuable insight without any interaction from the analyst.
- In cases where the initial layout does not give enough clarity or when an analyst wants to view things differently, a few nodal mouse-drag position adjustments can provide a much faster method of exposing insightful relationships and clusters.

The following behaviors and characteristics are now part of the graph:

- Entities of similar types tend to cluster together visually.

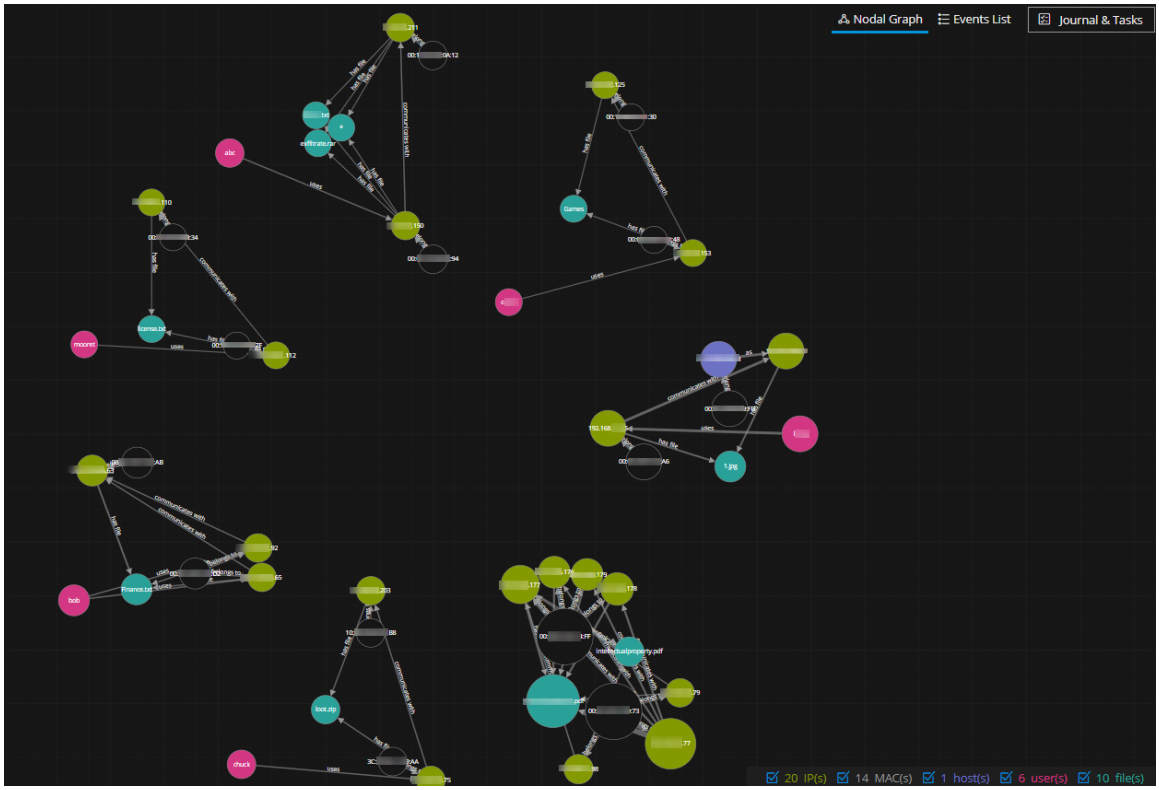


- Attributes and actions are better differentiated. Arrows that represent attributes ("as", "is named", "belongs to", and "has file") tend to be shorter than those representing actions ("call" and "communicates with").



- Leaf nodes, which are nodes that only have a single relationship to a single entity, tend to stay closer together.

- Disjointed graphs, such as clusters of entities and relationships that do not have connections with one another, are forced apart.



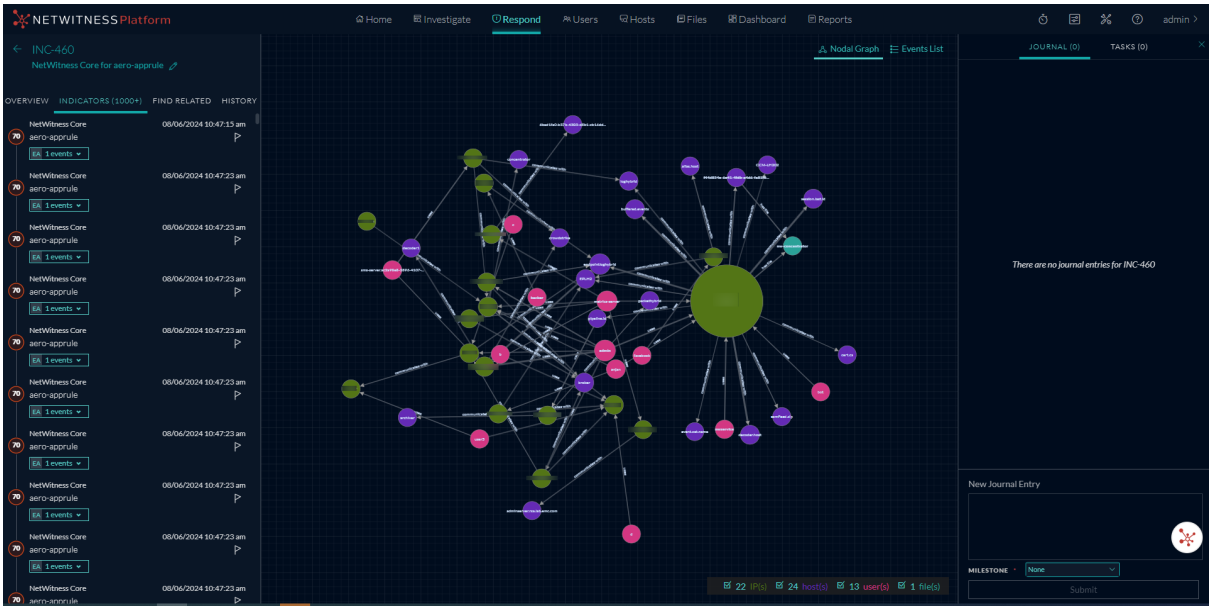
Dragged nodes are pinned in place. Double-click a node to unpin it and allow the forces to apply again to the node.

Select Node Types to View on the Nodal Graph

Note: This option is available in NetWitness Platform Version 11.2 and later.

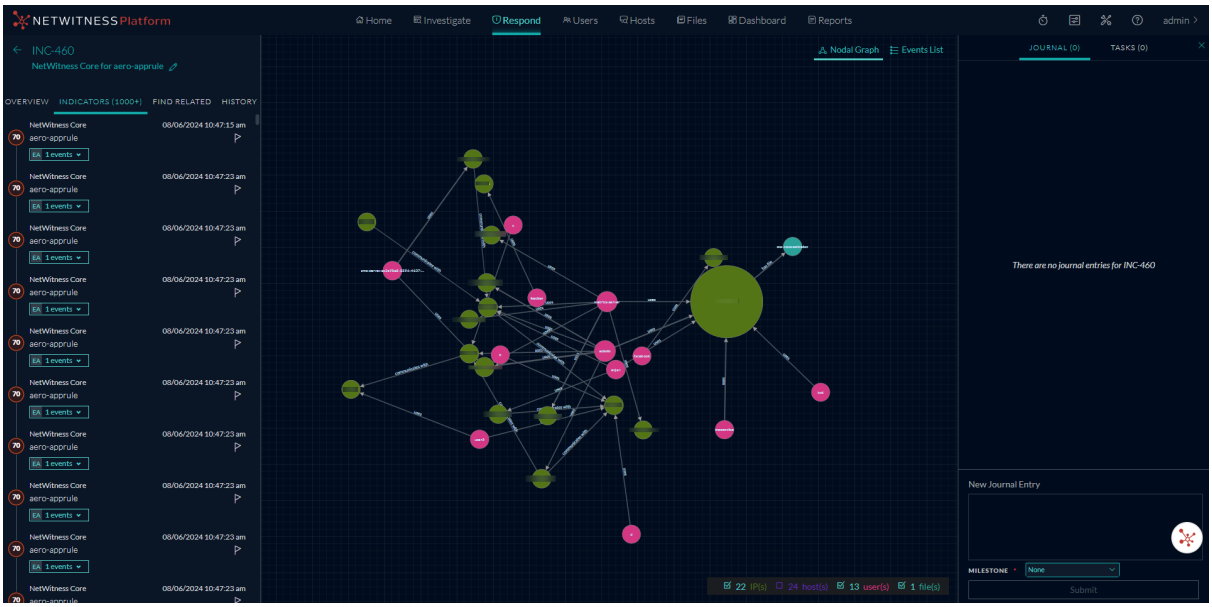
In the Incident Details view nodal graph, you can hide node types to further study the interactions between the entities on the nodal graph.

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.
   If you do not see the nodal graph, click Nodal Graph.

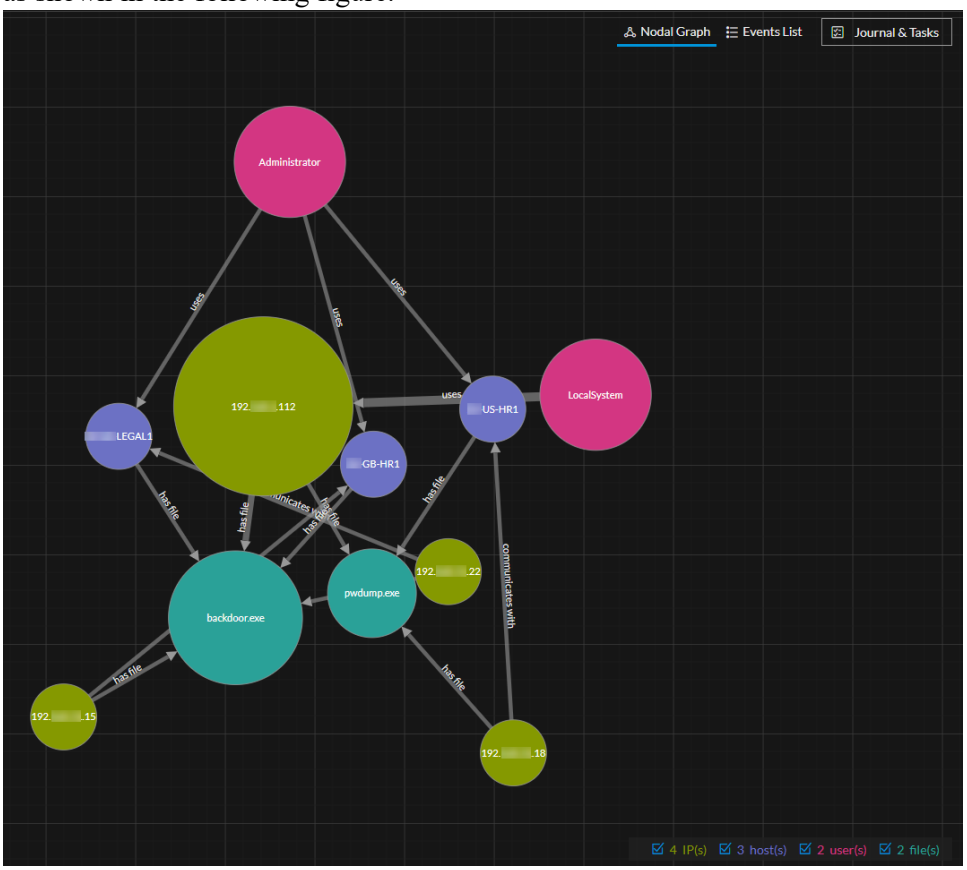


3. To hide node types, in the legend, clear the checkbox for the node types that you would like to hide in the nodal graph.

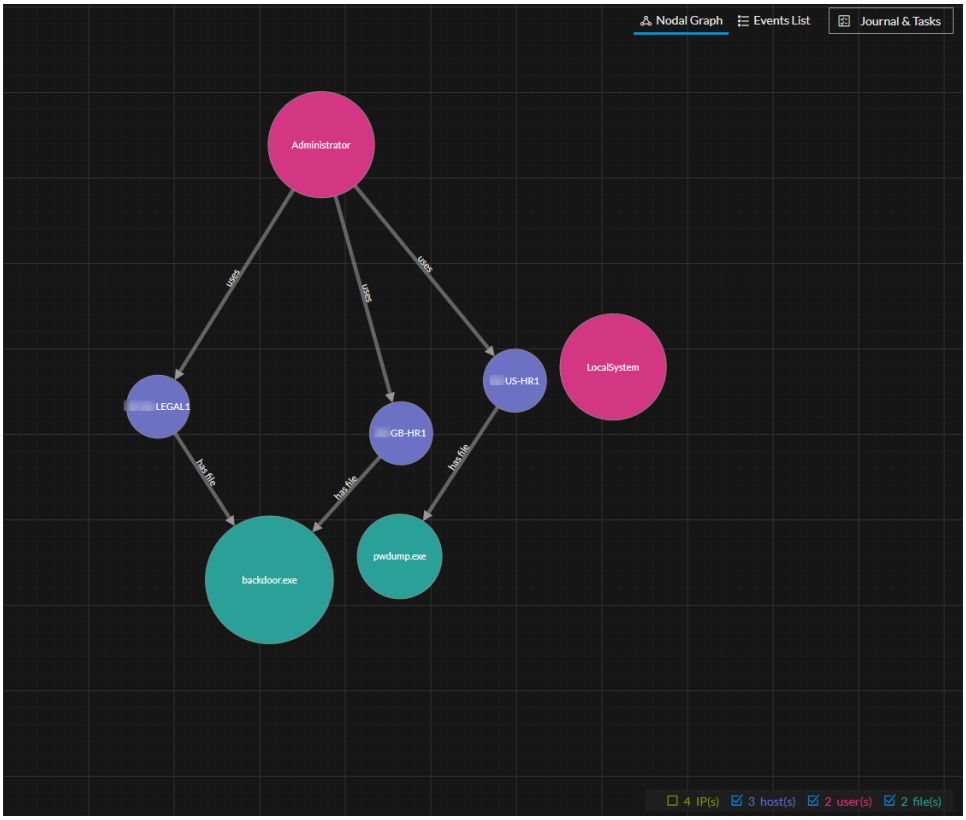
   The following example shows the IP address node type cleared and the IP address nodes are now hidden.



4. 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 has overlapping entity relationships as shown in the following figure.



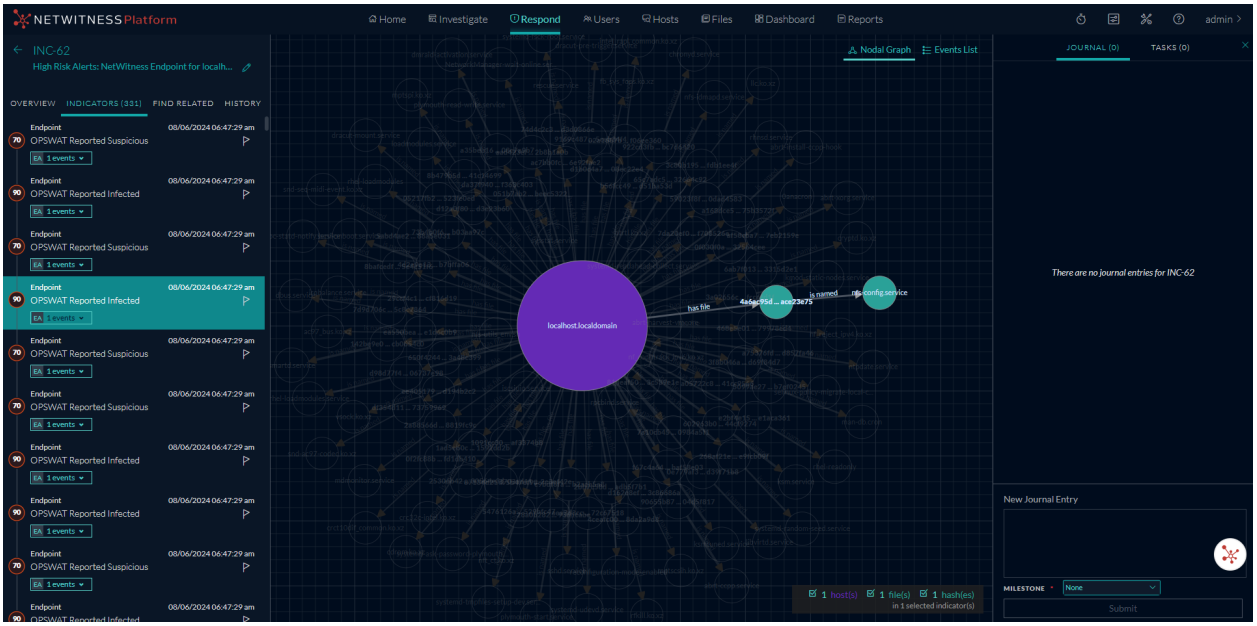
After hiding the IP node types, you can get a better understanding of what is happening with the remaining nodes.



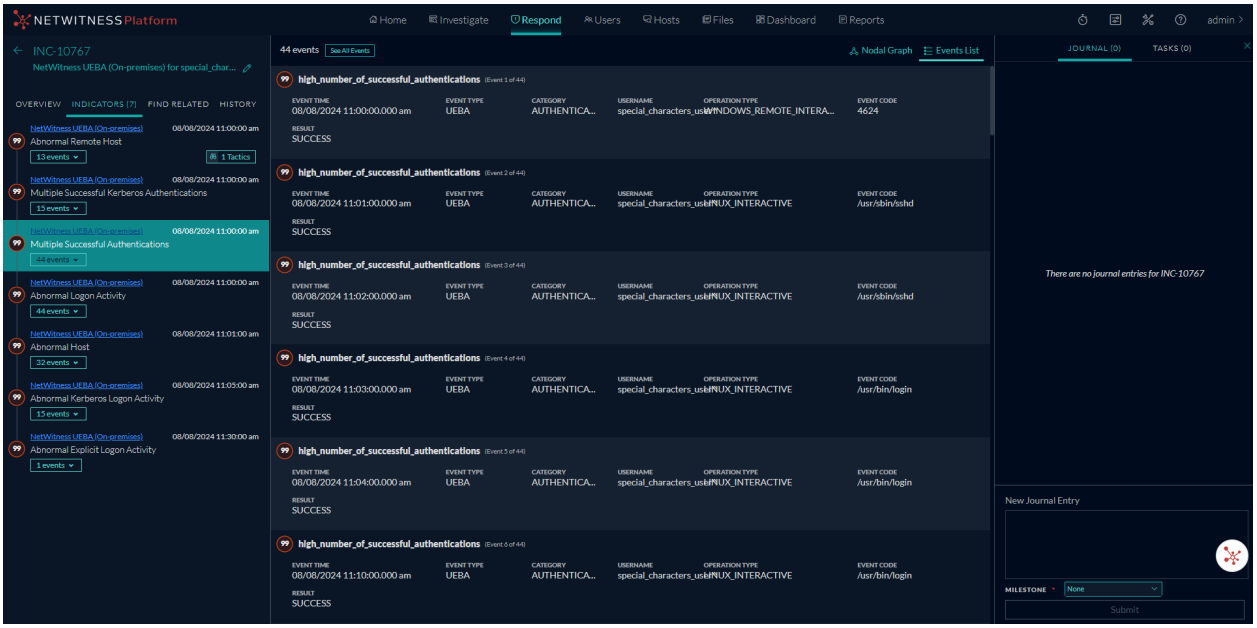
Filter the Data in the Incident Details View

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.



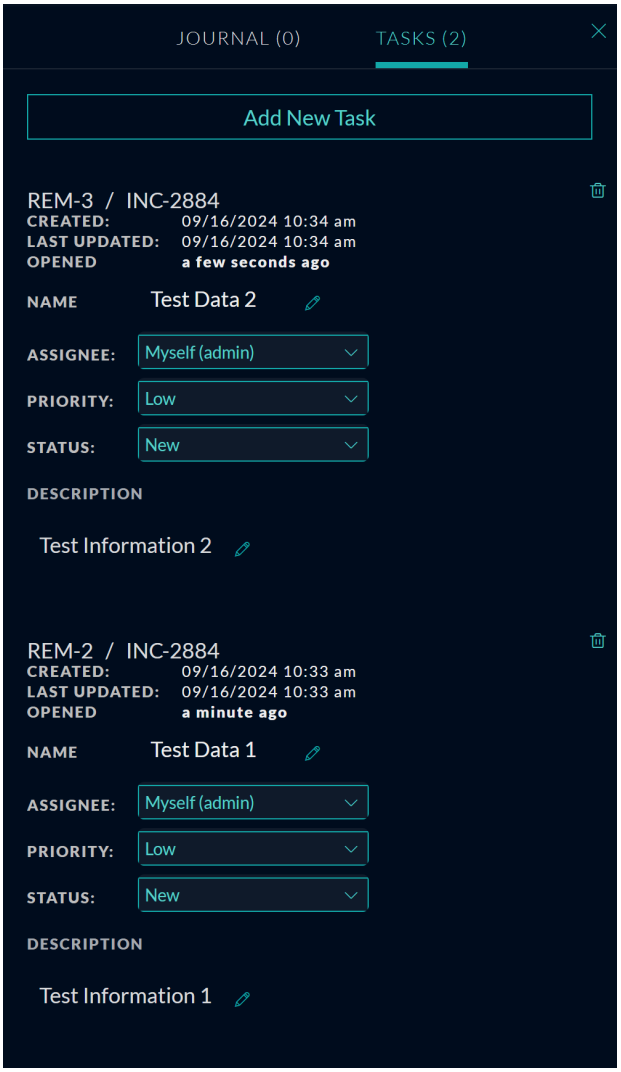
If you select an indicator to filter the Events List, only the events for that indicator are shown in the list. The following figure shows an indicator selected that contains forty-four events. The filtered Events List shows those forty-four events.



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.
3. In the Journal on the right side of the Incident Details view, click the **TASKS** tab.
   If you cannot see the Journal, click **Journal & Tasks** and then click the **TASKS** tab.
   The Tasks panel shows all of the tasks for the incident.

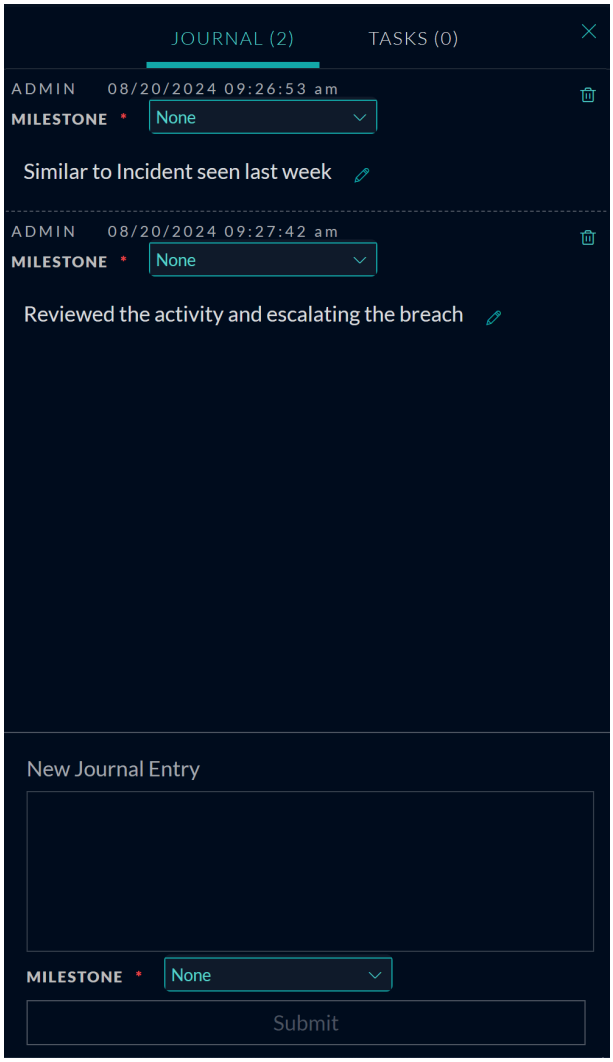


For more information about tasks, see Tasks List View, View All Incident Tasks, and Create a Task.

View Incident Notes

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

1. Go to **Respond > Incidents** and locate the incident that you want to view in the Incidents List.
2. Click the link in the **ID** or **NAME** field of the incident.
   The Journal on the right side of the Incident Details view shows all of the journal entries for the incident.
   If you cannot see the Journal, in the toolbar, click **Journal & Tasks**.

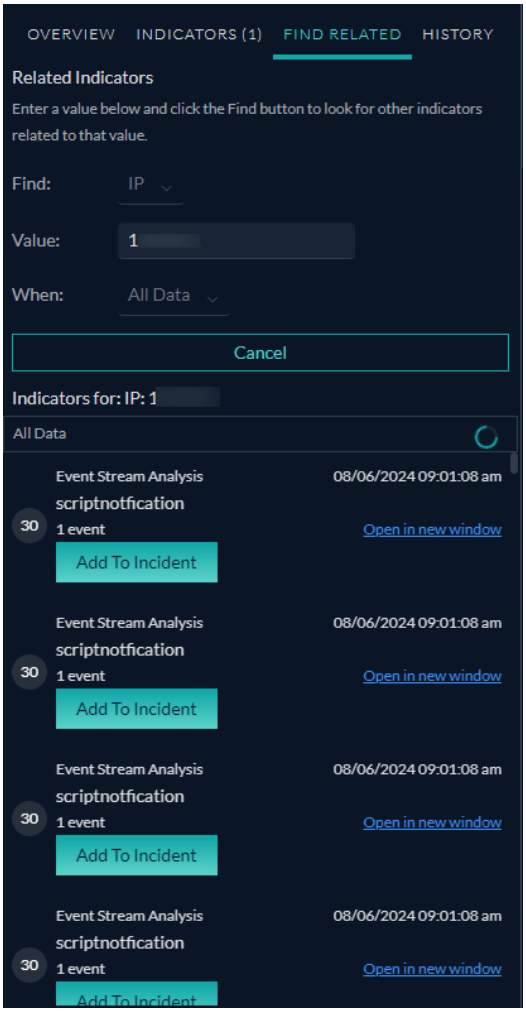


Find Related Indicators

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.

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.
3. In the left panel of the Incident Details view, click the **FIND RELATED** tab.
   The Related Indicators panel is displayed.



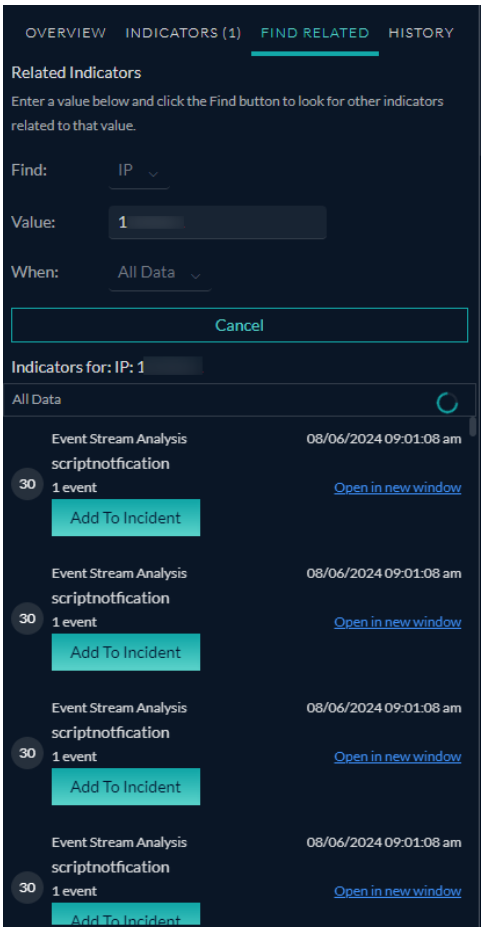
4. In the **Find** field, select the entity type to search, such as IP.
5. In the **Value** field, type a value for the entity, such as a specific IP address.

6. In the **When** field, select the time period to search, such as the Last 24 Hours.
7. 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.

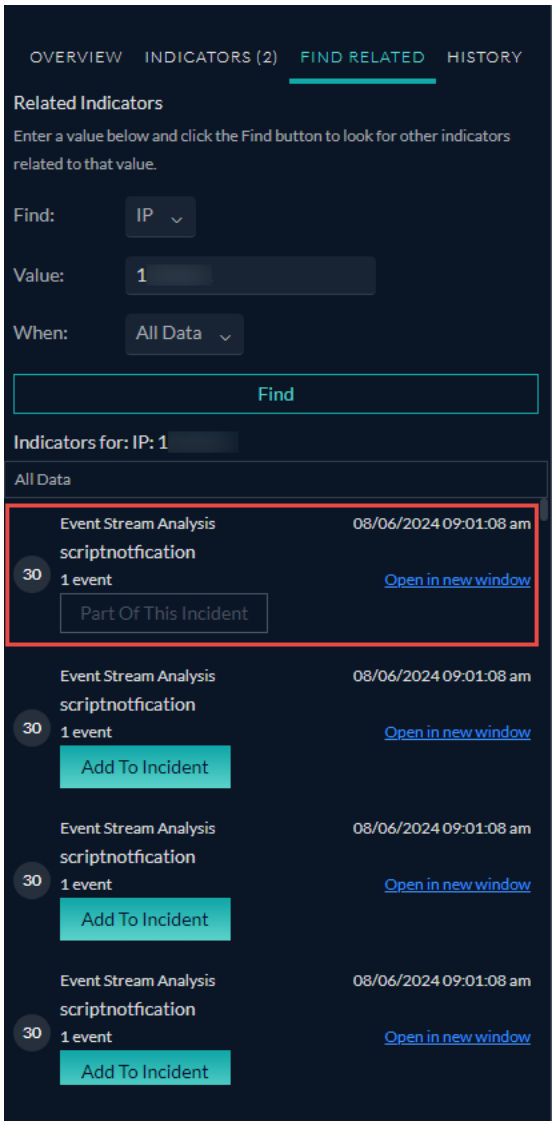
Add Related Indicators to the Incident

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.

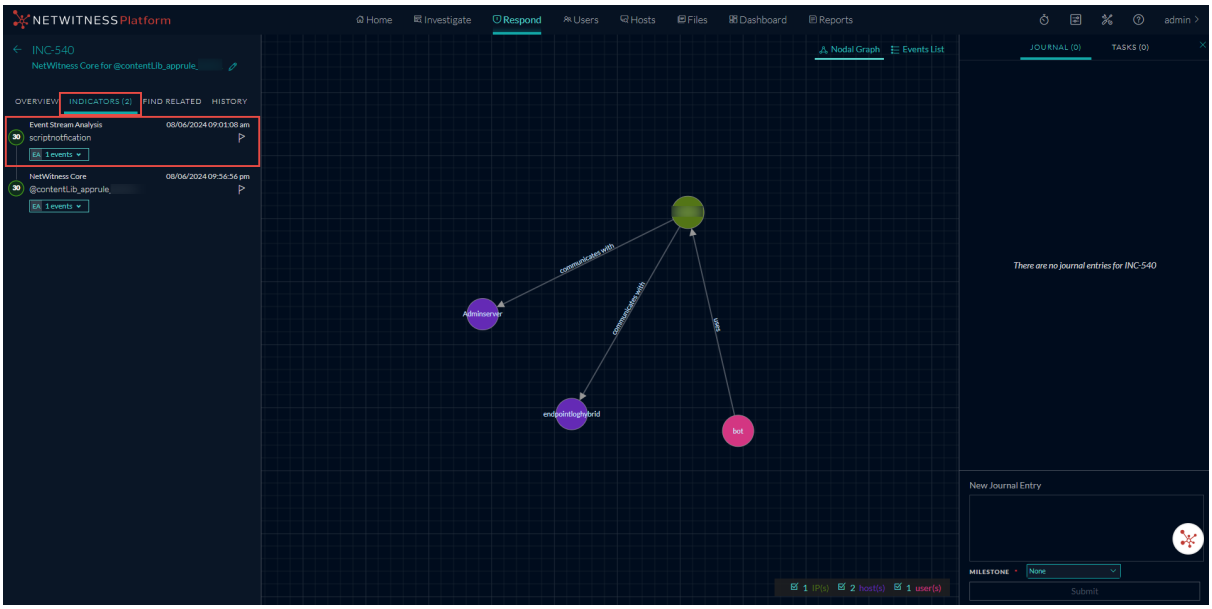
1. In the Related Indicators panel, do a search to find related indicators. See Find Related Indicators above.



2. Review the alerts in the search results. The **Indicators for** section (below the Find button) lists the related indicators (alerts).
3. 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.
4. For each alert that you want to add to the current incident as a related indicator, click the **Add to Incident** button.
   The button in the Related Indicators panel now shows **Part of This Incident**.



The selected related indicator adds to the Indicators panel. The Indicators tab now shows the additional indicator.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
INC-540
NetWitness Core for @contentLib_apprule_
OVERVIEW
INDICATORS (2)
FIND RELATED
HISTORY
Event Stream Analysis
08/06/2024 09:01:08 am
scriptnotfication
1 events
NetWitness Core
08/06/2024 09:56:56 pm
@contentLib_apprule_
1 events
Nodal Graph
Events List
communicates with
communicates with
uses
Adminserver
endpointloghybrid
bot
1 IP(s)
2 host(s)
1 user(s)
JOURNAL (0)
TASKS (0)
There are no journal entries for INC-540
New Journal Entry
MILESTONE
None
Submit

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.

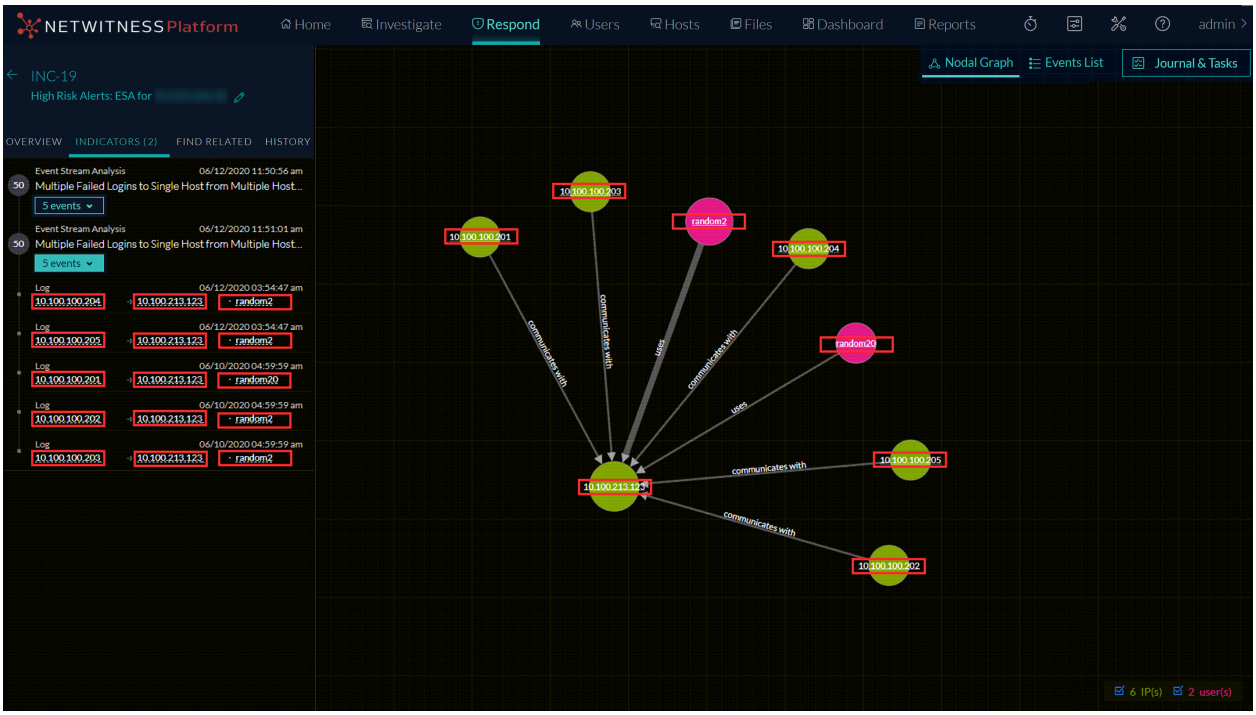
You can perform the following procedures to further investigate an incident:

- View Contextual Information
- Add an Entity to a Whitelist
- Create a List
- View the Reputation Status of a File Hash
- Pivot to the Investigate > Events View
- Pivot to the Hosts or Files View
- 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

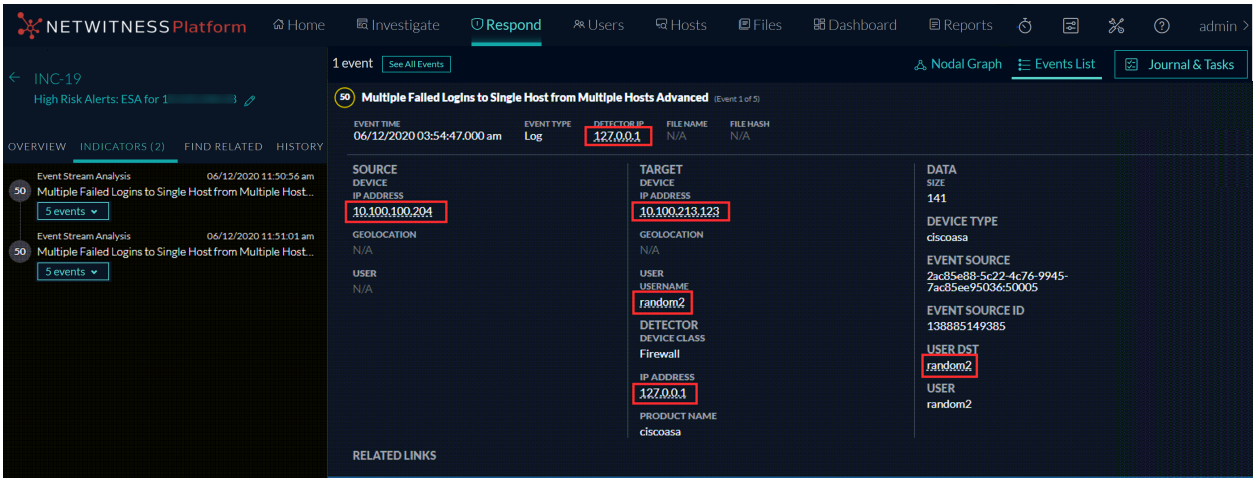
View Contextual Information

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



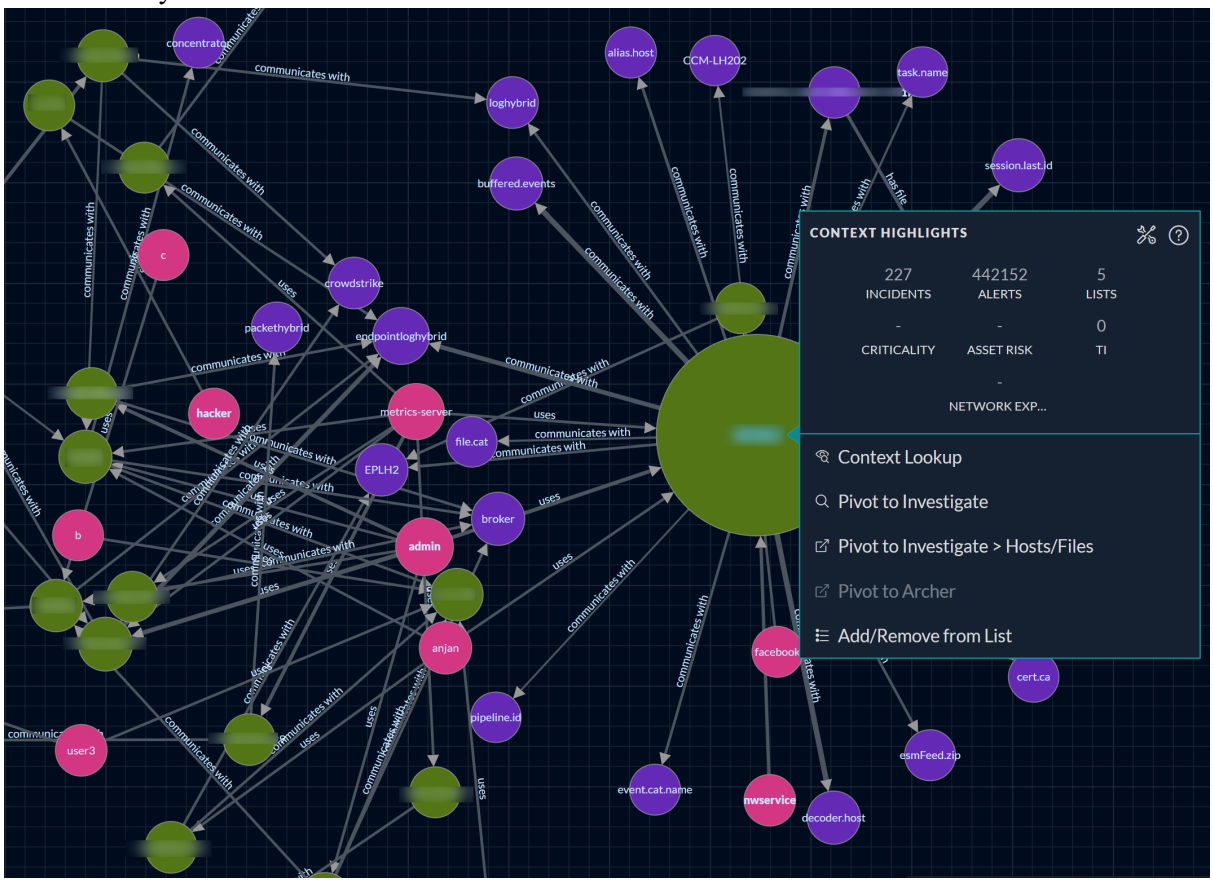
The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and NetWitness Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, NetWitness 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).

Note: The **contexthub-server.contextlookup.read** permission is enabled only for Administrators, Analysts, Malware Analysts, SOC Managers and Respond Administrators. Administrators can enable this permission for other roles in the **Respond** view to view context lookup for meta values and perform the Add/Remove from List actions. For more information, see the "Role Permissions" topic in the *System Security and User Management Guide*.

To view contextual information:

1. In the Indicators panel, Events List, or the Nodal Graph, left or right-click 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 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//, Criticality, Asset Risk, Reputation, and Threat Intelligence (TI). Depending on your data, you may be able to click these items for more information.

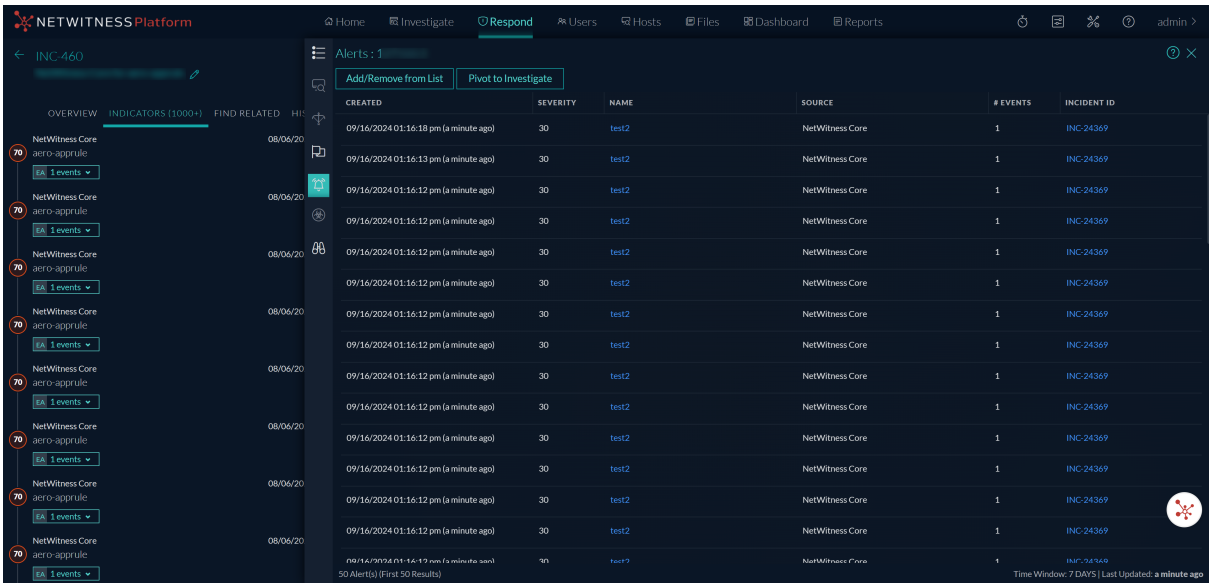
   TI information comes from the STIX data source configured in Context Hub. For more information,

see the *Context Hub Configuration Guide*.
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 Archer configuration is enabled and configured properly.

For more information, see Pivot to the Investigate > Events View, Pivot to Archer, Pivot to NetWitness Endpoint Thick Client, Pivot to the Hosts or Files View, and Add an Entity to a Whitelist.

2. 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.

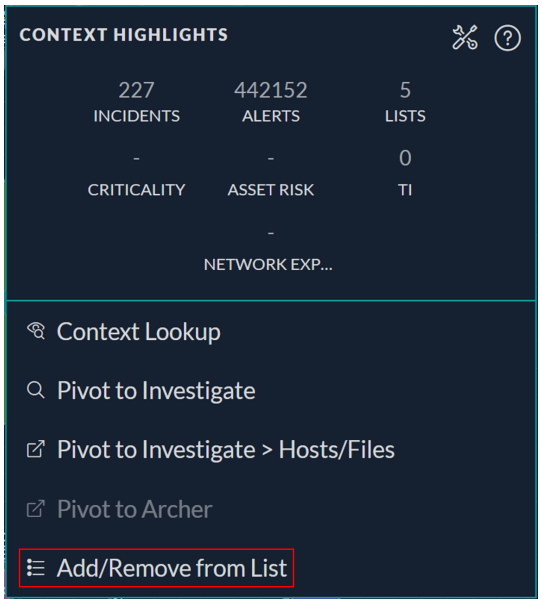


   To understand the different views within the Context Hub Lookup panel, see Context Lookup Panel - Respond View.

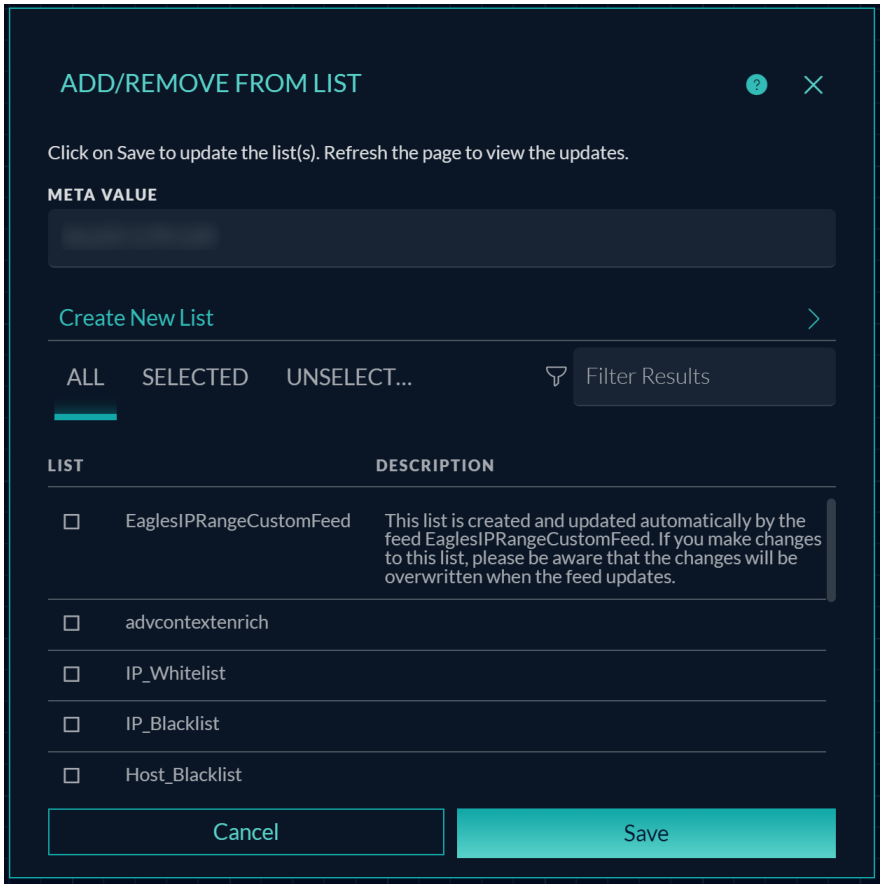
Add an Entity to a Whitelist

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

1. In the Indicators panel, Events List, or the Nodal Graph, left or right-click the underlined entity that you would like to add to a Context Hub list.
   A context tooltip appears showing the available actions.



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



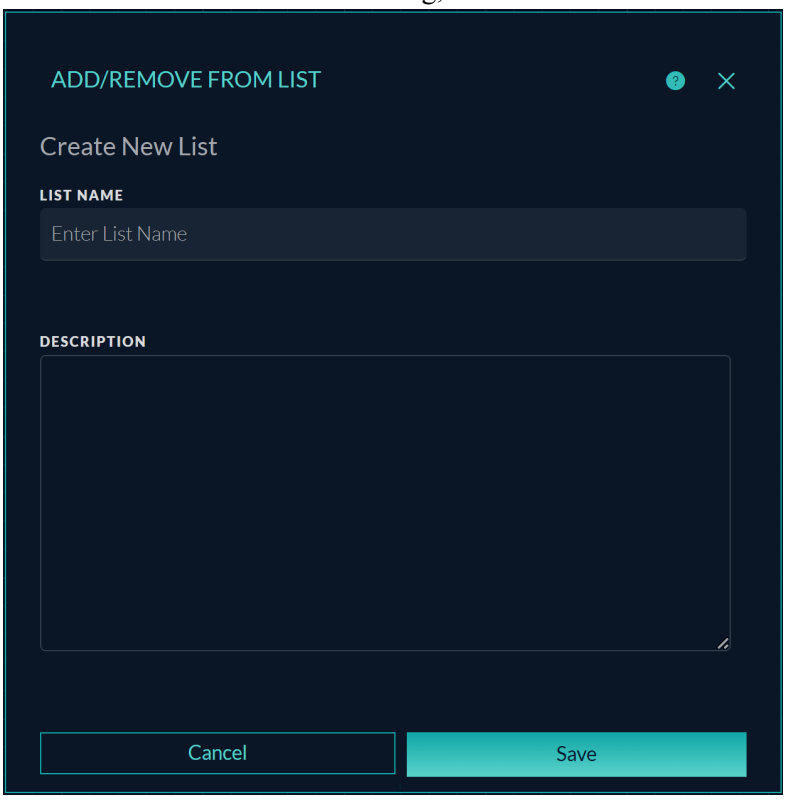
3. Select one or more lists and click **Save**.
   The entity appears on the selected lists.
   Add/Remove from List Dialog provides additional information.

Create a List

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

To create a list in Context Hub:

1. In the Indicators panel, Events List, or the Nodal Graph, left or right-click the underlined entity that you would like to add to a Context Hub list.
   A context tooltip opens showing the available actions.
2. In the **Actions** section of the tooltip, click **Add/Remove from List**.
3. In the Add/Remove from List dialog, click **Create New List**.



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

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 in the Investigate and Respond views. In the 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.

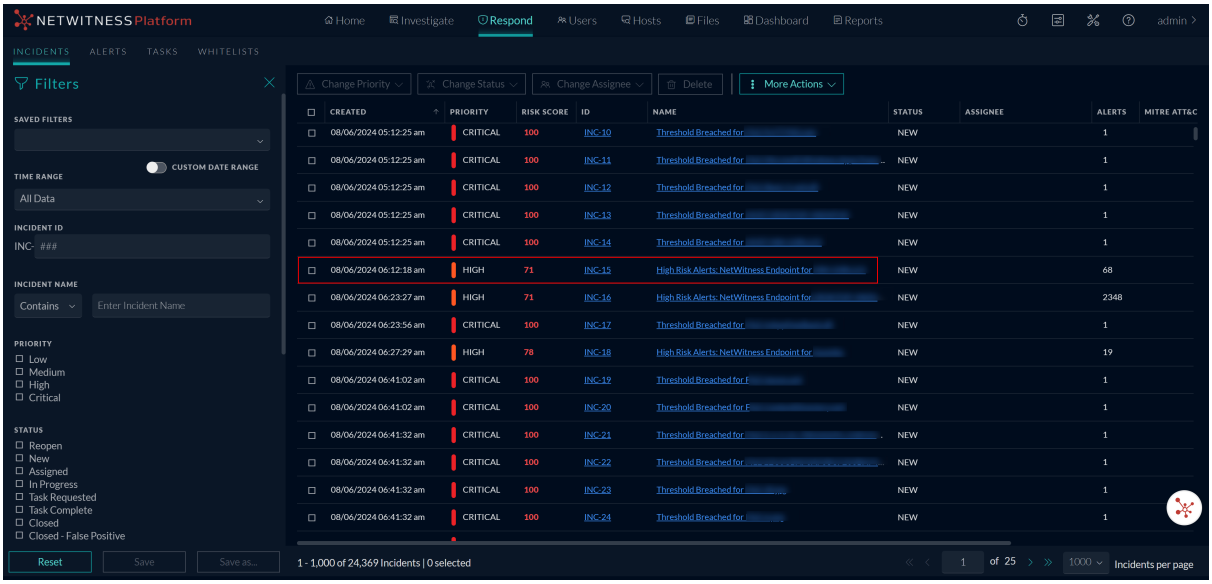
Reputation	Description
Malicious	File hash is labeled as malicious.
Suspicious	File hash is suspected to be malicious.
Unknown	File hash is not known.
Known	File hash information is known to the file reputation service and does not have any previous bad record.
Known Good	File hash information is known good, such as files signed by Microsoft or NetWitness.
Invalid	File hash format is invalid.

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

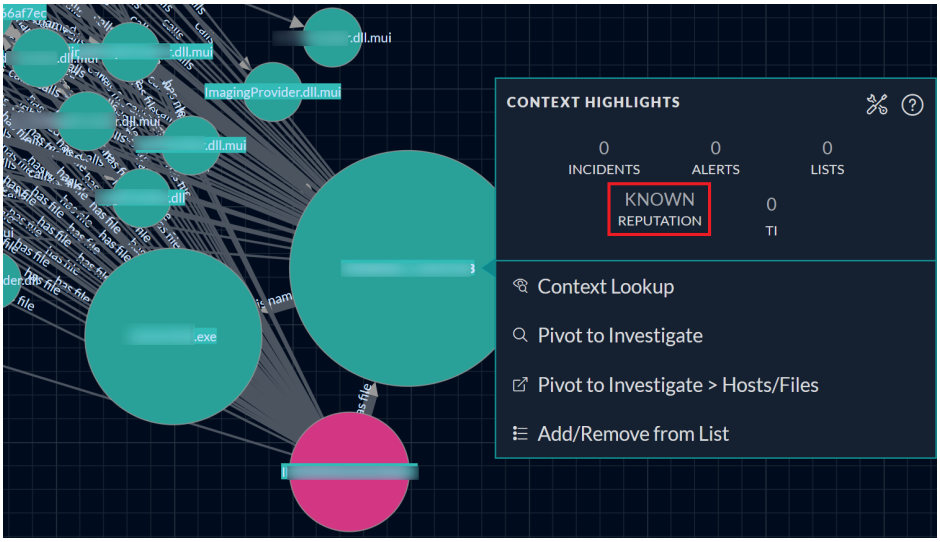
The suspicious or malicious files are available for further analysis in the **Investigate > Navigate** view and **Investigate > Events** view. For more information on the file reputation service, see the *Live Services Management Guide* and the *NetWitness Endpoint User Guide*.

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.



3. In the Incident Details view, left or right click the file hash entity.
The context tooltip displays the reputation status of the selected file hash entity.



4. Click **Reputation** to view the reputation status information.

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

Pivot to the Investigate > Events View

For a more thorough investigation of the incident, you can access the **Investigate** > **Events**.

1. In the Indicators panel, Events List, or the Nodal Graph, left or right click any underlined entity to access a context tooltip.
2. In the context tooltip panel, select **Pivot to Investigate**.
   The Events view opens, which enables you to perform a deep dive investigation.

For more information, see the *NetWitness Investigate User Guide*. For troubleshooting information with the Investigate > Events link see the *Alerting with ESA Correlation Rules User Guide*.

Pivot to the Hosts or Files View

For a more thorough investigation about specific Hosts and Files, you can access the 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 context tooltip panel, 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 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 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.

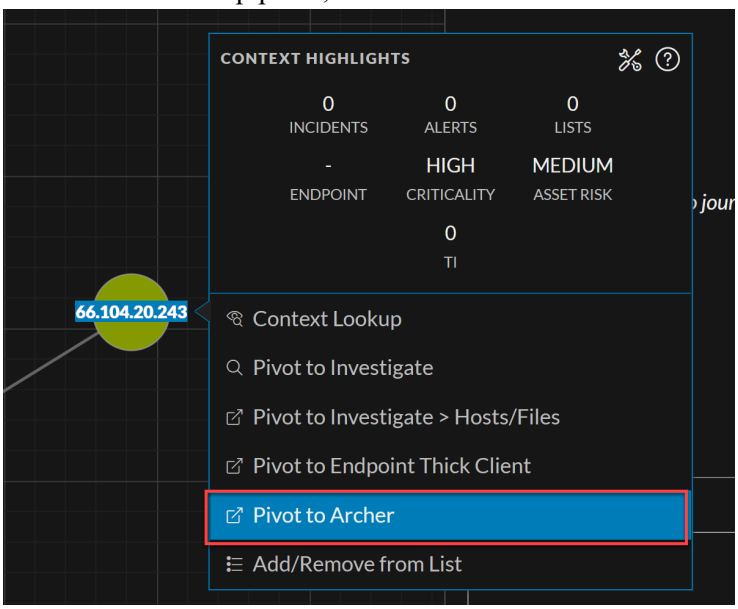
1. In the Indicators panel, Events List, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the context tooltip panel, select **Pivot to Endpoint Thick Client**.
   The NetWitness Endpoint thick client application opens outside of your web browser.

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

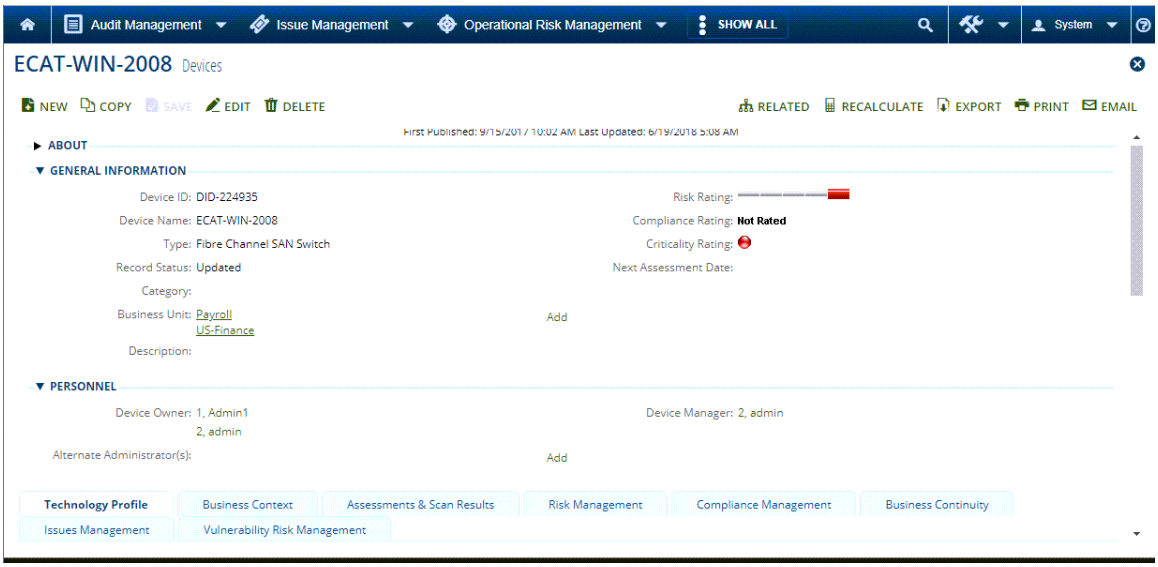
Pivot to Archer

For viewing more details about the device in 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, left or right click any underlined entity (IP address, host, and Mac address) to access a context tooltip.
2. In the context tooltip panel, select **Pivot to Archer**.



3. The device details page in **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 Archer configuration is enabled and configured properly.

For more information, see the *NetWitness 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 Events 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 Events panel. The Events panel in the Respond view shows the Events view from Investigate for specific indicator events. For detailed information about the Events view, see the *NetWitness Investigate User Guide*.

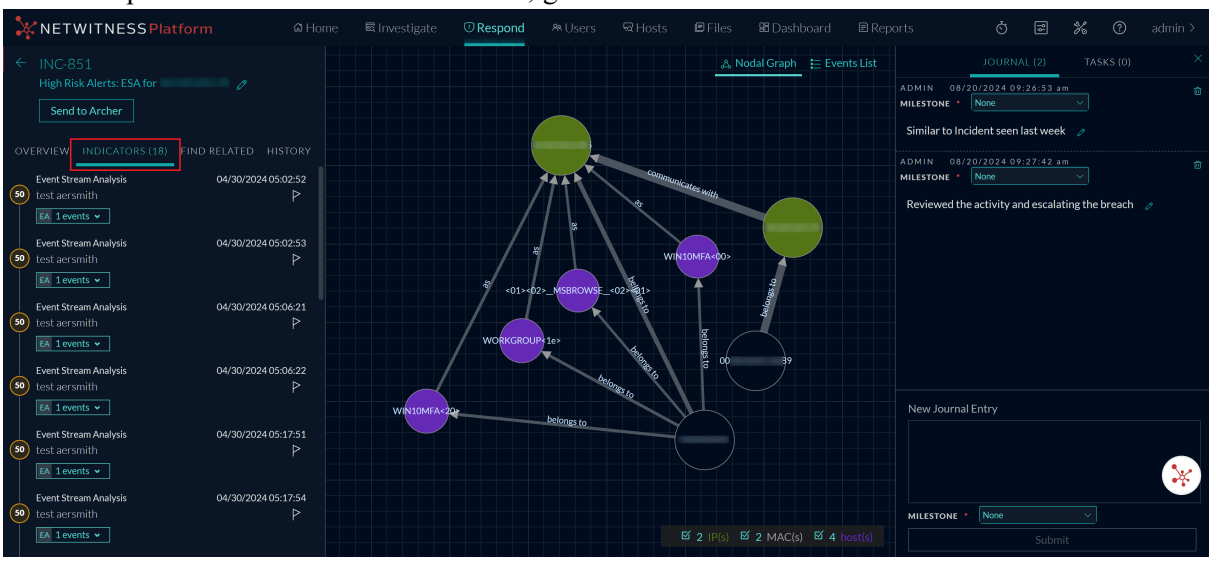
Note: You must have the following Investigate-server permissions to view the Events panel in the Respond view:
`event.read`
`content.reconstruct`
`content.export`
The Events view requires all Core services to be on NetWitness Platform 11.4 or later.

Migration Considerations

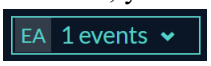
Migrated incidents from NetWitness versions before 11.2 will not show the Events panel in the Respond Incident Details view Indicators panel. Likewise, if you use alerts that were migrated from versions before 11.2 to create incidents in 11.5, you will also not be able to view the Events panel in the Respond view for those incidents.

To access event analysis details for an event in the Indicators panel:

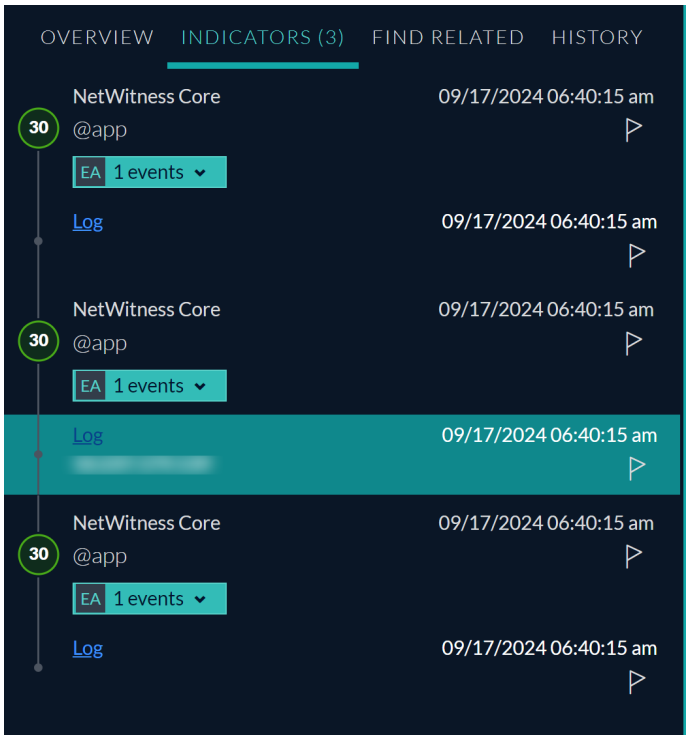
1. Go to **Respond > Incidents**.
2. In the Incidents List view, choose an incident to view and then click the link in the **ID** or **NAME** column for that incident.
   The Incident Details view is displayed.
3. In the left panel of the Incident Details view, go to the **Indicators** tab.



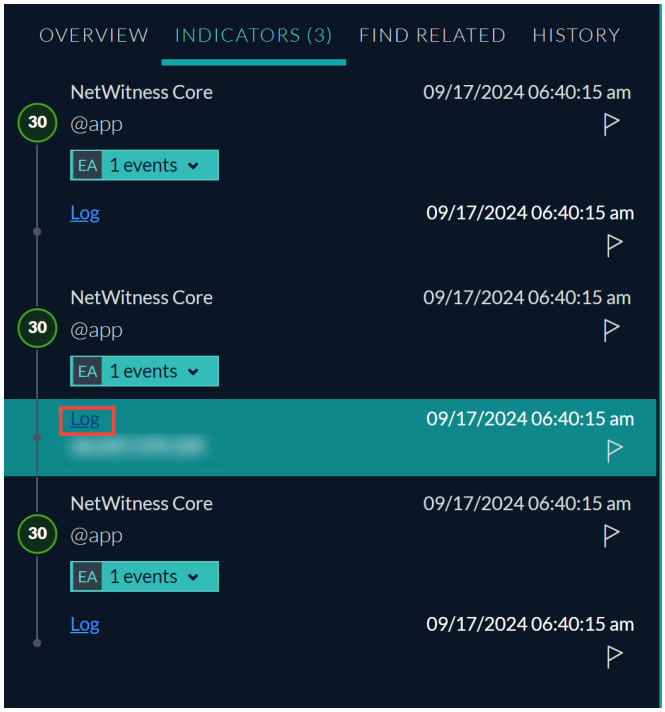
Data source information is shown above the names of the indicators. You can also see the creation date and time as well as the number of events in the indicator. If event analysis (EA) information is available, you can see an **EA** icon in front of the event count as shown in the following figure.



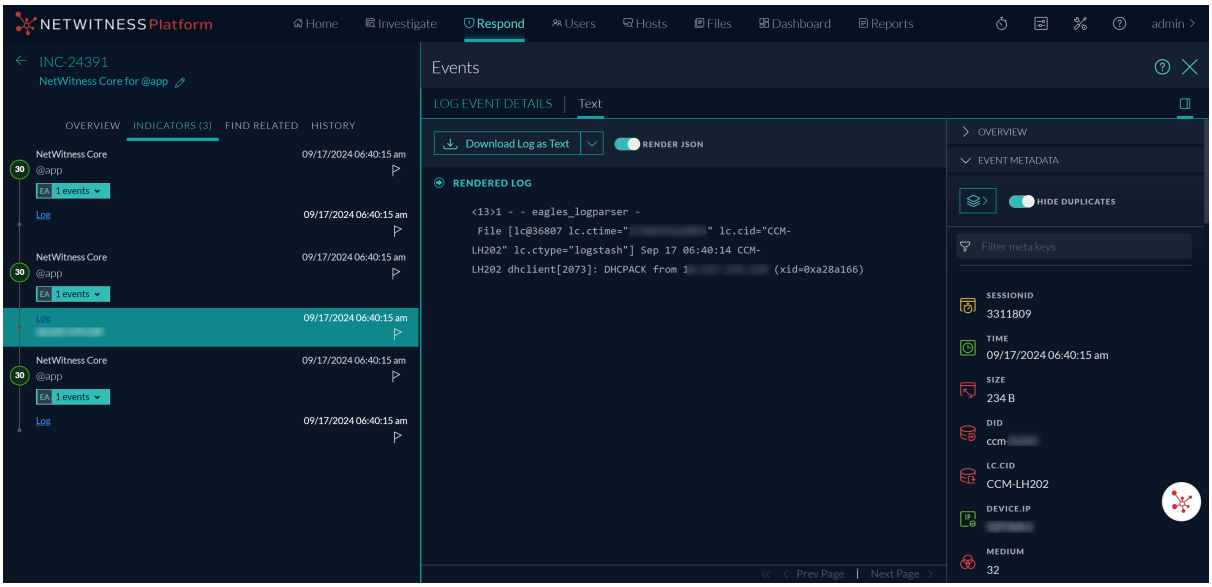
4. Click an event count with an **EA** icon to view additional event information.



5. Click an event type hyperlink within the event to open the Events panel. In the following example, the event type is Log.



The Events panel shows event details for the event, such as Log event details. The information available can vary based on the event type.

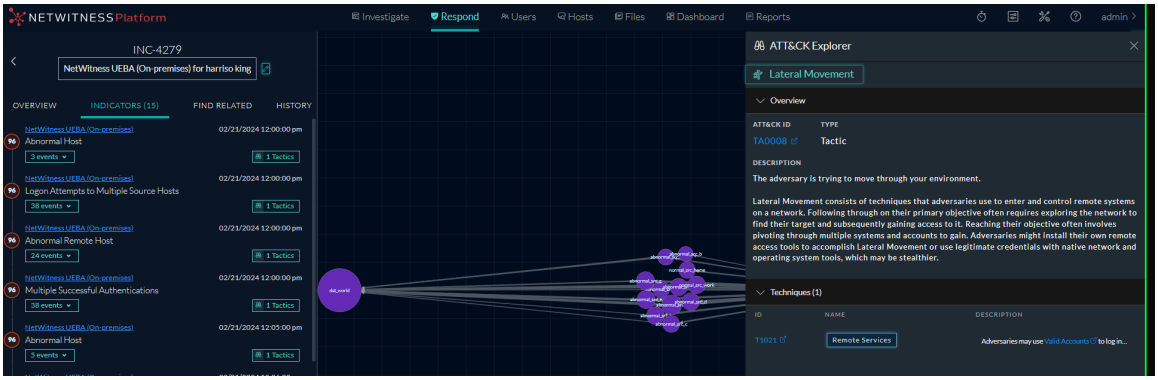


For detailed information about the Events view, see the *NetWitness Investigate User Guide*.

Note: If you want to send the Events URL link to another analyst, you can copy the event type hyperlink, for example Network.

View User Entity Behavior Analytics for Indicators

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*.

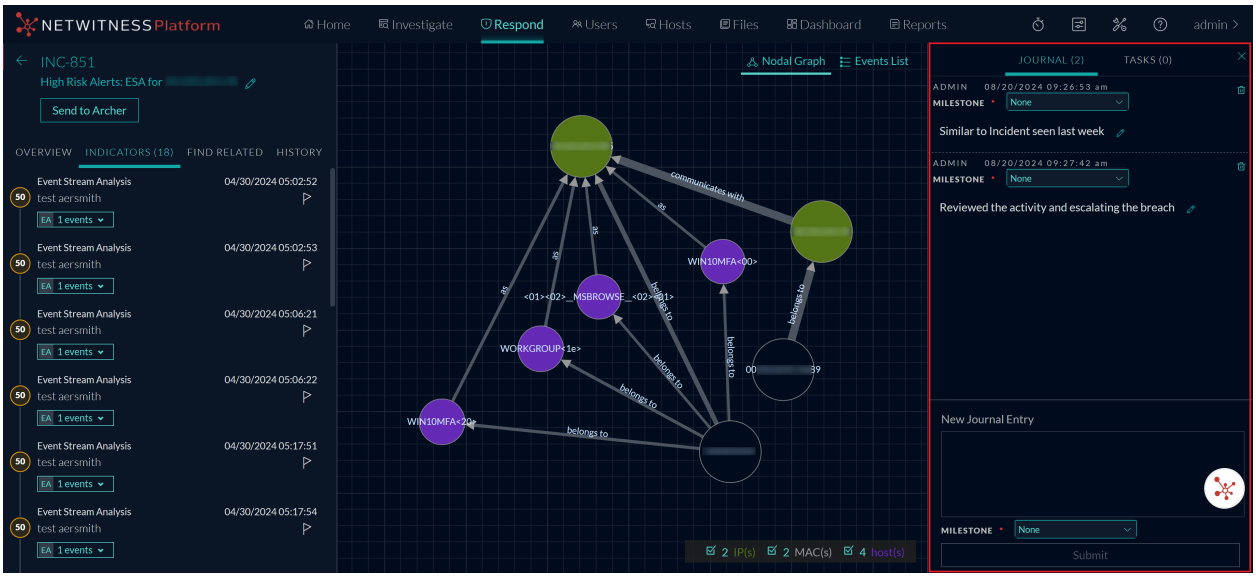


Document Steps Taken Outside of NetWitness

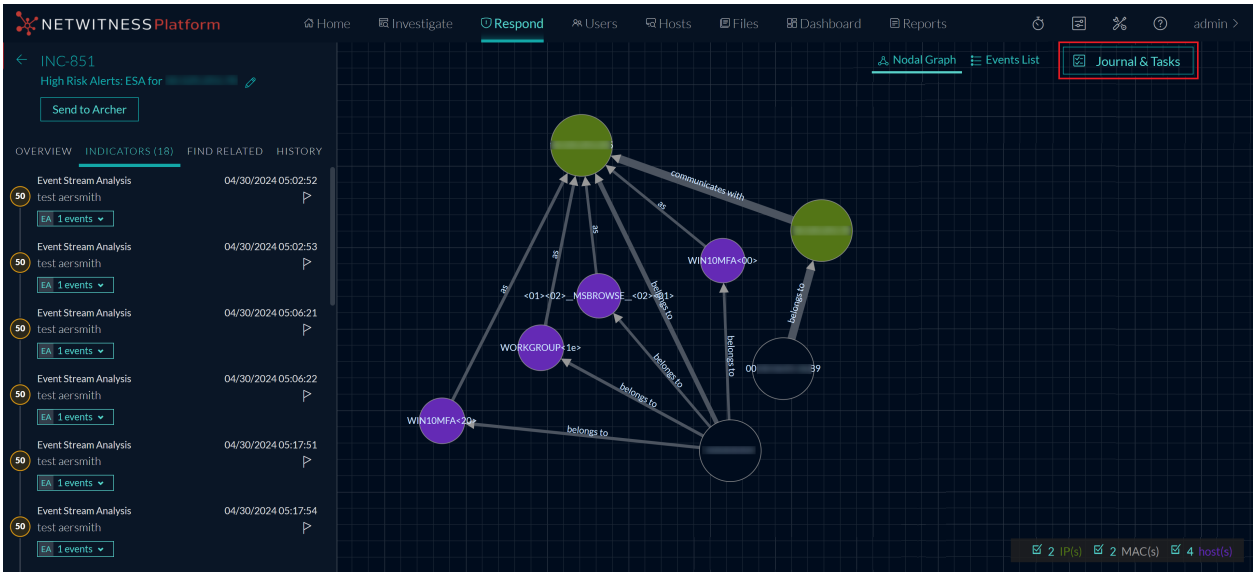
The journal shows notes added by analysts and it enables you to collaborate with your peers. You can post notes to a journal, add Investigation Milestone tags (Reconnaissance, Delivery, Exploitation, Installation, Command and Control, Action on Objective, Containment, Eradication, and Closure), and view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

View the Journal Entries for an Incident

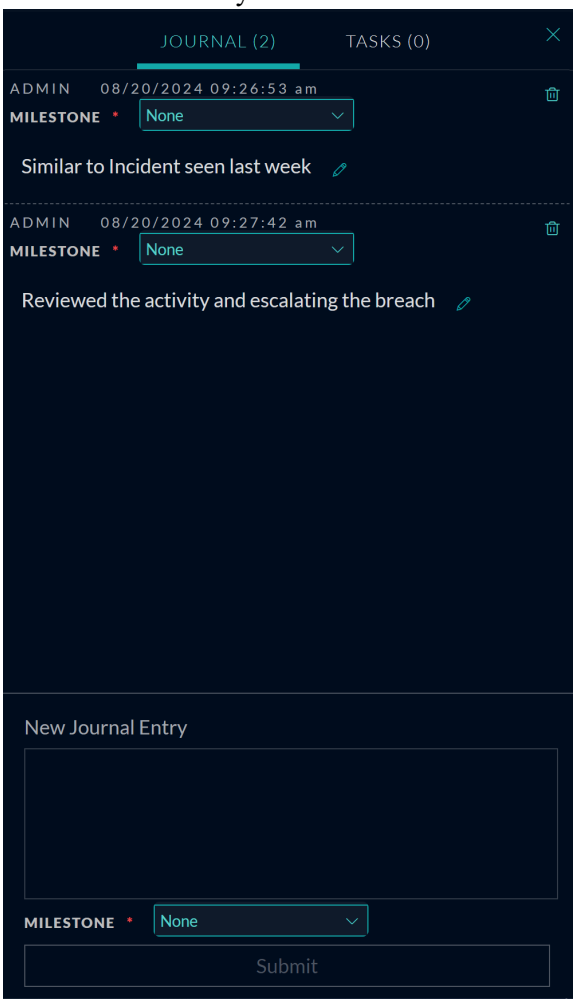
The Journal is on the right side of the Incident Details view.



If you do not see the Journal, in the toolbar, click **Journal & Tasks**.



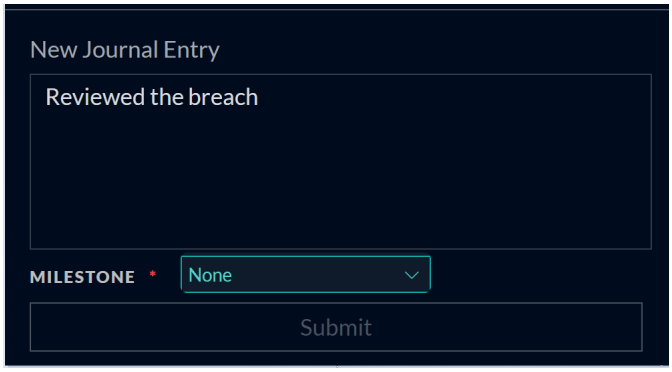
The Journal shows the history of activity on an incident. For each journal entry, you can see the author and time of the entry.



Add a Note

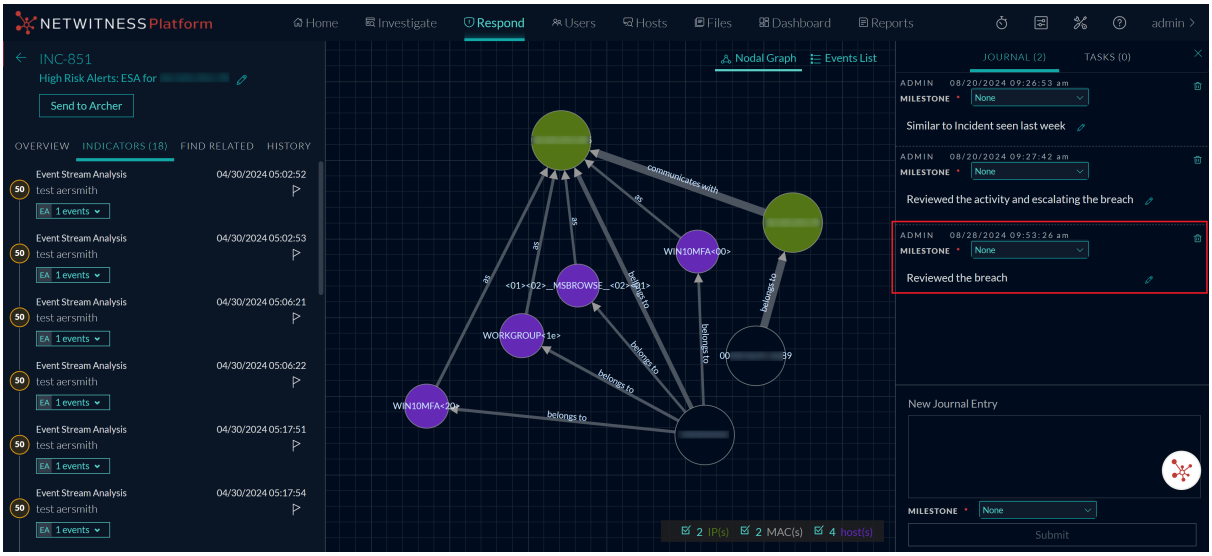
Typically, you will want to add a note to allow another analyst to understand the incident, or add a note for posterity so that your investigative steps are documented.

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



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

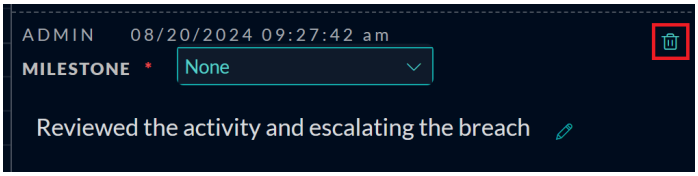
3. After you finish your note, click, **Submit**.
   Your new journal entry appears in the Journal.



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.

Use MITRE ATT&CK® Framework

MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. ATT&CK focuses on how external adversaries compromise and operate within computer information networks. It originated out of a project to document and categorize post-compromise adversary tactics, techniques and procedures (TTPs) against Microsoft Windows systems to improve detection of malicious behavior. It has since grown to include Linux and macOS, and has expanded to cover behavior leading up to the compromise of an environment, as well as technology-focused domains like mobile devices, cloud-based systems, and industrial control systems.

At a high-level, ATT&CK is a behavioral model that consists of the following core components.

- Tactics, denoting short-term, tactical adversary goals during an attack.
- Techniques, describing the means by which adversaries achieve tactical goals.
- Sub - techniques, describing more specific means by which adversaries achieve tactical goals at a lower level than techniques.
- Documented adversary usage of techniques, their procedures, and other metadata.

ATT&CK is organized in a series of technology domains, the ecosystem an adversary operates within. Currently, there are three technology domains:

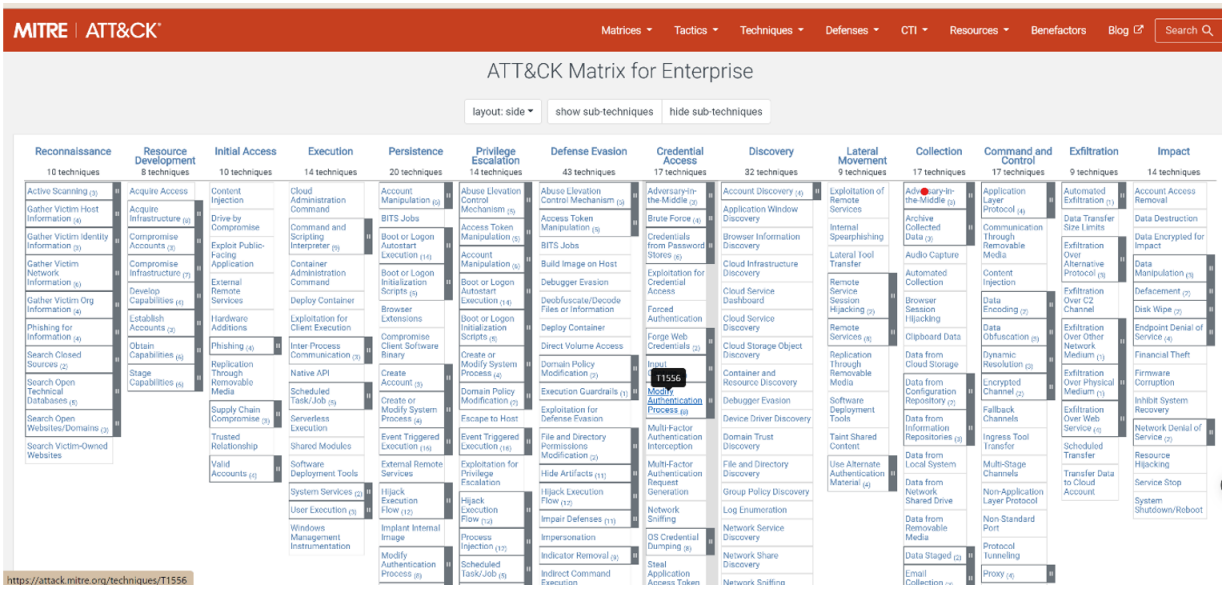
- ATT&CK for Enterprise: This iteration focuses on adversarial behavior in Windows, Mac, Linux, and Cloud environments.
- ATT&CK for Mobile: This iteration focuses on adversarial behavior on iOS and Android operating systems.
- ATT&CK for ICS: This iteration focuses on describing the actions an adversary may take while operating within an ICS network.

Within each domain are platforms, which may be an operating system or application, for example, Microsoft Windows. Techniques and sub-techniques can apply to multiple platforms.

The ATT&CK Model

The basis of ATT&CK is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives. Those objectives are represented by the tactic categories the techniques and sub-techniques fall under. This relatively simple representation strikes a useful balance between sufficient technical detail at the technique level and the context around why actions occur at the tactic level.

The ATT&CK Matrix provides the relationship between tactics, techniques, and sub-techniques can be visualized in the ATT&CK Matrix. For example, under the Persistence tactic (this is the adversary's goal – to persist in the target environment), there are a series of techniques including Hijack Execution Flow, Pre-OS Boot, and Scheduled Task/Job. Each of these is a single technique that adversaries may use to achieve the goal of persistence. Furthermore, some techniques can be broken down into sub-techniques that describe in more detail how those behaviors can be performed. For example, Pre-OS Boot has three subtechniques consisting of Bootkit, Component Firmware, and System Firmware to describe how persistence is achieved before an operating system boots. Figure 2 depicts the Persistence Tactic with techniques and four techniques expanded to show sub-techniques: Account Manipulation, Pre-OS Boot, Scheduled Task/Job, and Server Software Component.



About Adversaries and Techniques

A cyber adversary is a person, group, organization, or government that conducts or has the intent to perform malicious actions against other cyber resources.

The adversaries use certain ways called Techniques and perform certain actions to achieve a tactical goal.

For example: The adversary uses **Access Token Manipulation** technique to modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.

For more information on Techniques, see https://attack.mitre.org/techniques/enterprise/.

There are 3 categories in Techniques:

- **Enterprise**: This Techniques category displays a total of 201 Techniques.

  For more information, see https://attack.mitre.org/techniques/enterprise/.

- **Mobile**: This Techniques category displays a total of 72 Techniques.

  For more information, see https://attack.mitre.org/techniques/mobile/.

- **ICS**: This Techniques category displays a total of 81 Techniques.

  For more information, see https://attack.mitre.org/techniques/ics/.

Tactics

Tactics represent the tactical goal of the adversary. They provide information about the reason for performing any action.

For example: If the Tactic name is **Reconnaissance**, it represents that the adversary may want to achieve credential access.For more information on Tactics, see https://attack.mitre.org/tactics/enterprise/.

There are 3 categories in Tactics:

- **Enterprise**: This Tactics category displays a total of 14 Tactics.

  For more information, see https://attack.mitre.org/tactics/enterprise/.

- **Mobile**: This Tactics category displays a total of 14 Tactics.

  For more information, see https://attack.mitre.org/tactics/mobile/.

- **ICS**: This Tactics category displays a total of 12 Tactics.

  For more information, see https://attack.mitre.org/tactics/ics/.

Sub -Techniques

Sub-techniques are the multiple ways that an adversary uses to execute the main Technique. In specific, Sub-technique is a way to describe a specific implementation of a technique in more detail. These Sub-techniques are more detailed adversary actions.

For example: The technique such as **Phishing** has 4 sub-techniques which provide more details about how adversaries send phishing messages to gain access to systems.

There are 424 Sub-techniques listed under the Enterprise Techniques list. For more information, see https://attack.mitre.org/techniques/enterprise/.

There are 42 Sub-techniques listed under the Mobile Techniques list. For more information, see https://attack.mitre.org/techniques/mobile/.

There are no Sub-techniques listed under the ICS Techniques list.

Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

For example: The Mitigation **Audit** represents performing audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

There are 43 Mitigations listed under Enterprise Mitigations list. For more information, see https://attack.mitre.org/mitigations/enterprise/.

There are 12 Mitigations listed under Mobile Mitigations list. For more information, see https://attack.mitre.org/mitigations/mobile/.

There are 52 Mitigations listed under ICS Mitigations list. For more information, see https://attack.mitre.org/mitigations/ics/.

Procedure Examples

A procedure is the specific details of how an adversary carries out a technique to achieve a tactic.

For example: MITRE ATT&CK lists how an adversary APT19 (G0073) uses a watering hole attack to perform a **Drive-by Compromise** (Technique **T1189**) and gain **Initial Access** (Tactic **TA0001**) of **forbes.com** in 2014.

For more information on Procedure Examples, see https://attack.mitre.org/resources/faq/#faq-0-2-header and https://attack.mitre.org/groups/G0032/.

Note: NetWitness Platform uses **ATT&CK for Enterprise**.

MITRE ATT&CK Integration with NetWitness Platform

MITRE ATT&CK is integrated with NetWitness Platform to help analysts look into the various techniques and tactics associated with the Incidents, alerts, and events. The new **ATT&CK© Explorer Panel** introduced in the **Respond** and **Investigate** view allows you to view the detailed information on the Tactics, Techniques, Sub - Techniques, Mitigations, and Procedure Examples associated with the Incidents, alerts, and events in the **Respond** and **Investigate** view.

NetWitness Live is integrated with MITRE framework to help analysts to view the MITRE ATT&CK Tactics and MITRE ATT&CK Techniques associated with the **Application Rules** and **Event Stream Analysis Rules**.

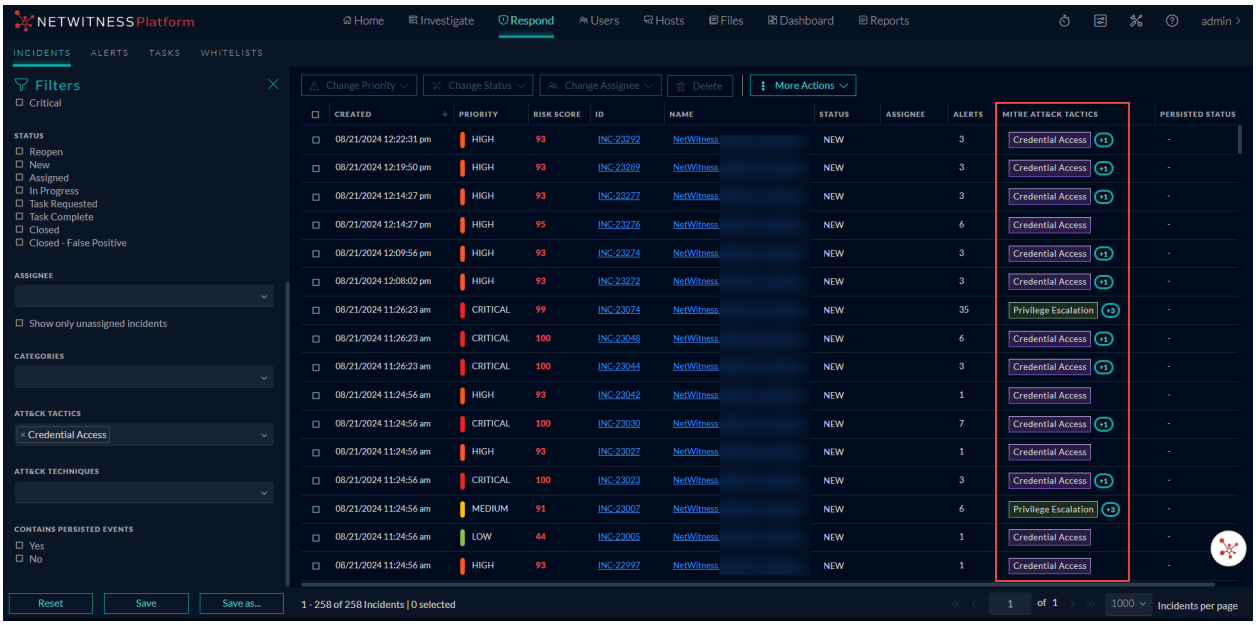
The Service Details Right panel ( (**Configure**) > **Policies** > **Content** > **Content Library** > **Application Rule** or **Event Stream Analysis Rule** > click a row > Service Details Right panel) is enhanced to provide information about the MITRE ATT&CK Tactics and MITRE ATT&CK Techniques. You can tag MITRE ATT&CK Tactics, Techniques, and Sub - Techniques while creating a custom **Application Rule** or **Event Stream Analysis Rule**.

For more information on MITRE ATT&CK integration in the Investigate view, see NetWitness *Investigate User Guide for 12.4*.

For more information on MITRE ATT&CK integration in CCM, see *Policy-based Centralized Content Management Guide for 12.4*.

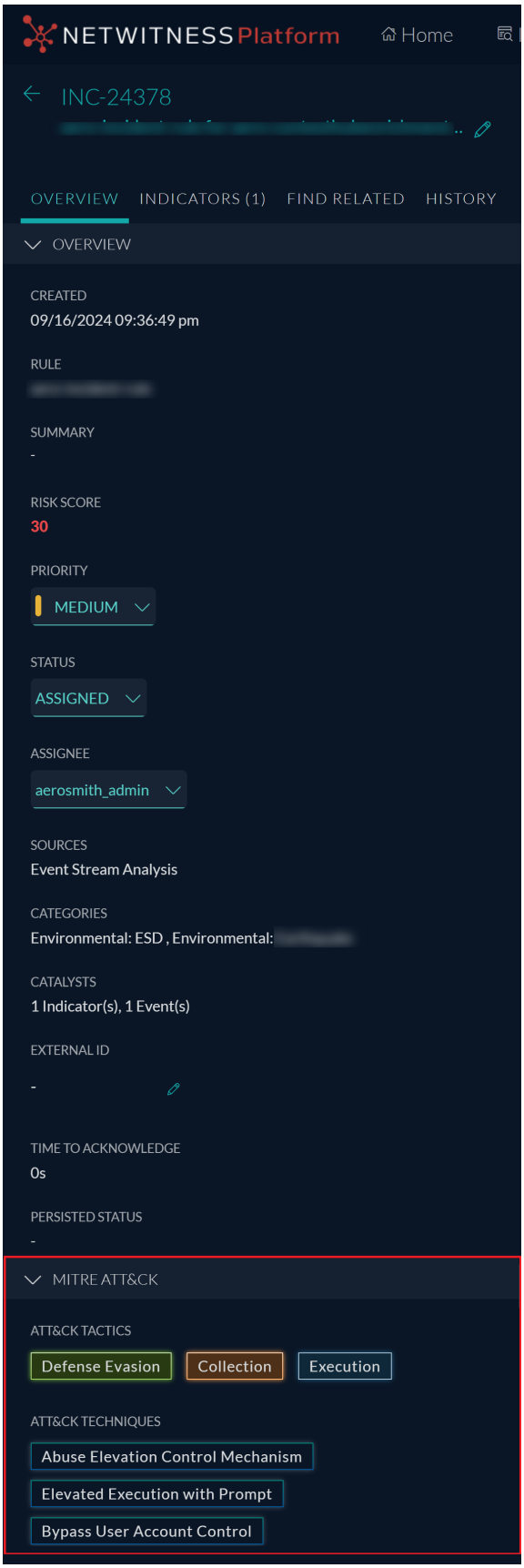
Incident List View Enhancement

In 12.4, the **Incident List** view is enhanced with **MITRE ATT&CK Tactics** column to display the particular Tactic associated with each Incident. The new **ATT&CK© Explorer** Panel populates when you click any Tactic in the **MITRE ATT&CK Tactics** column.



Incident Overview Panel Enhancement

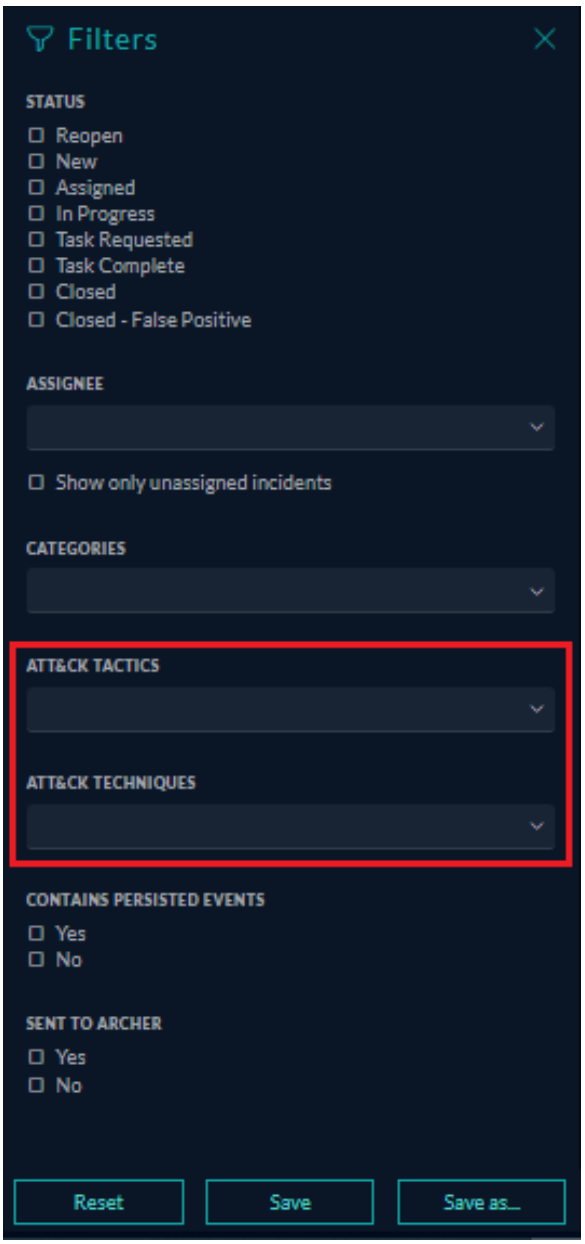
In 12.4, the **Incident Overview** Panel is enhanced with **MITRE ATT&CK Tactics** and **MITRE ATT&CK Techniques** field. Refer the following figure.


NETWITNESS Platform
Home
INC-24378
OVERVIEW
INDICATORS (1)
FIND RELATED
HISTORY
OVERVIEW
CREATED
09/16/2024 09:36:49 pm
RULE
SUMMARY
-
RISK SCORE
30
PRIORITY
MEDIUM
STATUS
ASSIGNED
ASSIGNEE
aerosmith_admin
SOURCES
Event Stream Analysis
CATEGORIES
Environmental: ESD , Environmental:
CATALYSTS
1 Indicator(s), 1 Event(s)
EXTERNAL ID
-
TIME TO ACKNOWLEDGE
0s
PERSISTED STATUS
-
MITRE ATT&CK
ATT&CK TACTICS
Defense Evasion
Collection
Execution
ATT&CK TECHNIQUES
Abuse Elevation Control Mechanism
Elevated Execution with Prompt
Bypass User Account Control

The new **ATT&CK© Explorer** Panel populates when you click the Tactic or Technique in the **Incident Overview** Panel.

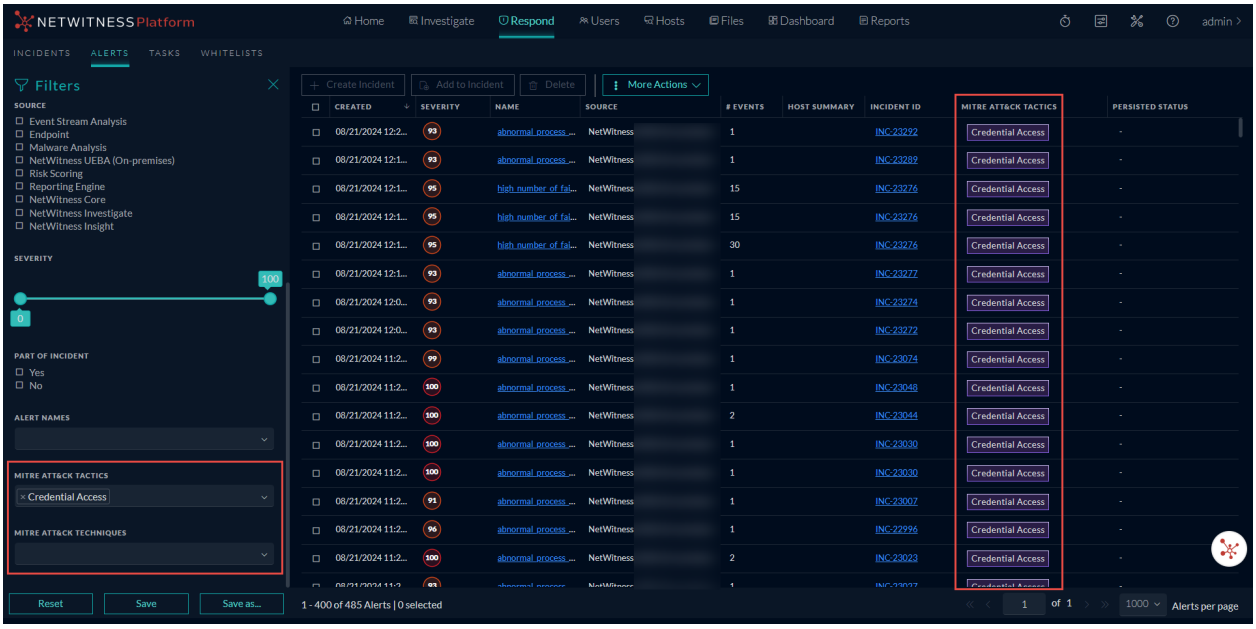
Incident Filters Panel Enhancement

In 12.4, the **Incident Filters** panel is enhanced with the new filters **MITRE ATT&CK TACTICS** and **MITRE ATT&CK TECHNIQUES**. You can filter the Incidents on the basis of the MITRE ATT&CK Tactics and Techniques associated with them. Refer the following figure.



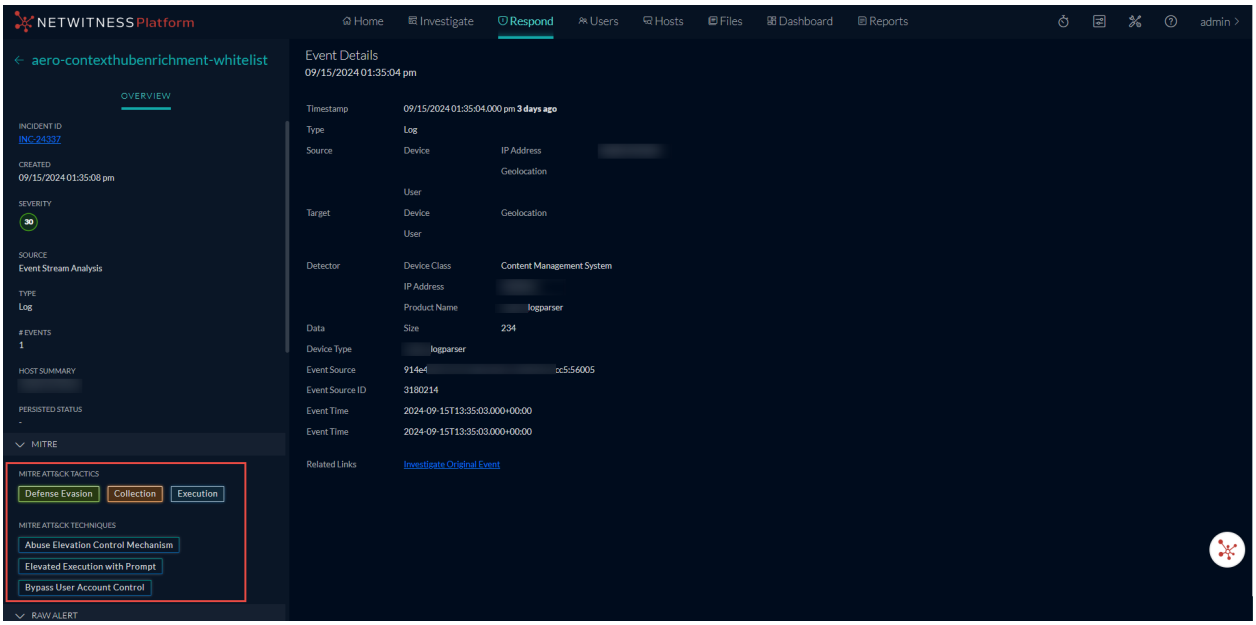
Alerts List View Enhancement

In 12.4, **Alerts List** view is enhanced with **MITRE ATT&CK Tactics** column to display the particular Tactic associated with each alert. The new **ATT&CK© Explorer** Panel populates when you click any Tactic in the **MITRE ATT&CK Tactics** column.



Alerts Details View Enhancement

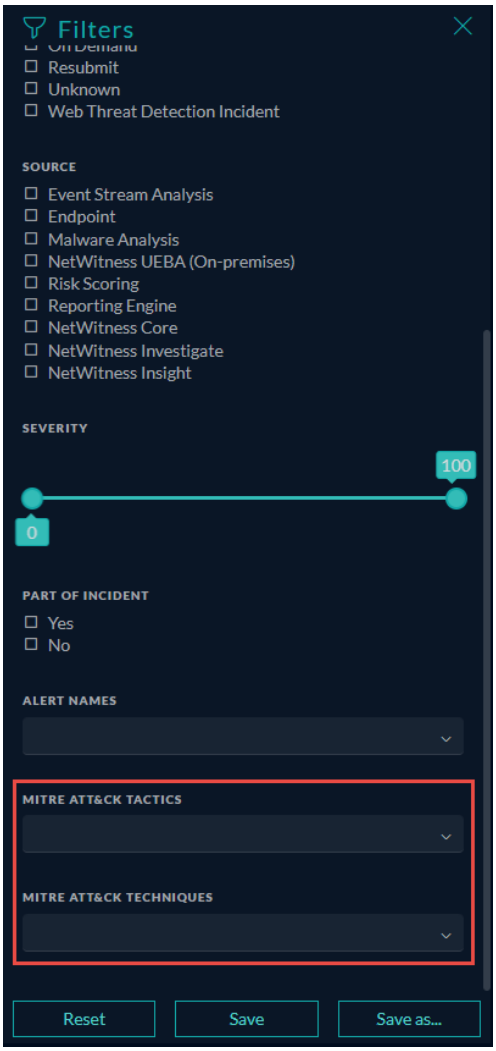
In 12.4, the **Overview** panel in the **Alerts Details** view is enhanced with **MITRE ATT&CK Tactics** and **MITRE ATT&CK Techniques** field.



The new **ATT&CK© Explorer** Panel populates when you click any Tactic or Technique in the **Overview** panel in **Alerts Details** view.

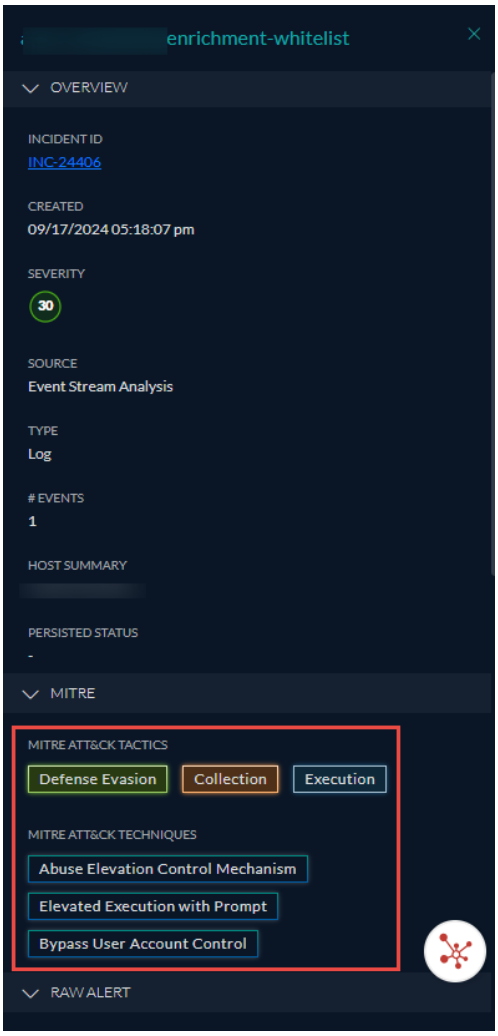
Alerts Filters Panel Enhancement

In 12.4, the **Alerts Filters** panel is enhanced with the new filters **MITRE ATT&CK TACTICS** and **MITRE ATT&CK TECHNIQUES**. You can filter the alerts on the basis of the MITRE ATT&CK Tactics and Techniques associated with them. Refer the following figure.



Alert Overview Panel Enhancement

In 12.4, the **Alert Overview** Panel is enhanced with **MITRE ATT&CK Tactics** and **MITRE ATT&CK Techniques** field. Refer the following figure.



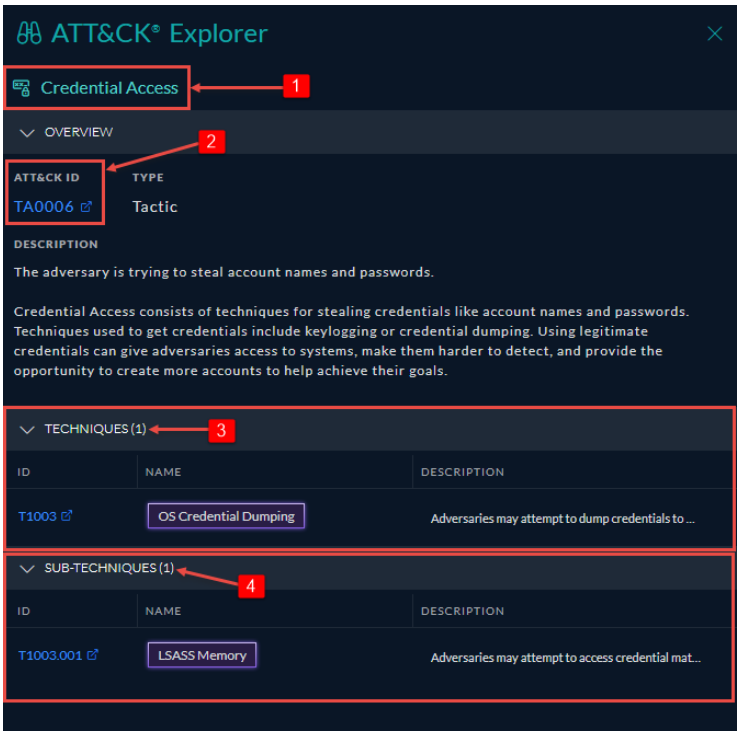
The new **ATT&CK© Explorer** Panel populates when you click the Tactic or Technique in the **Alert Overview** Panel.

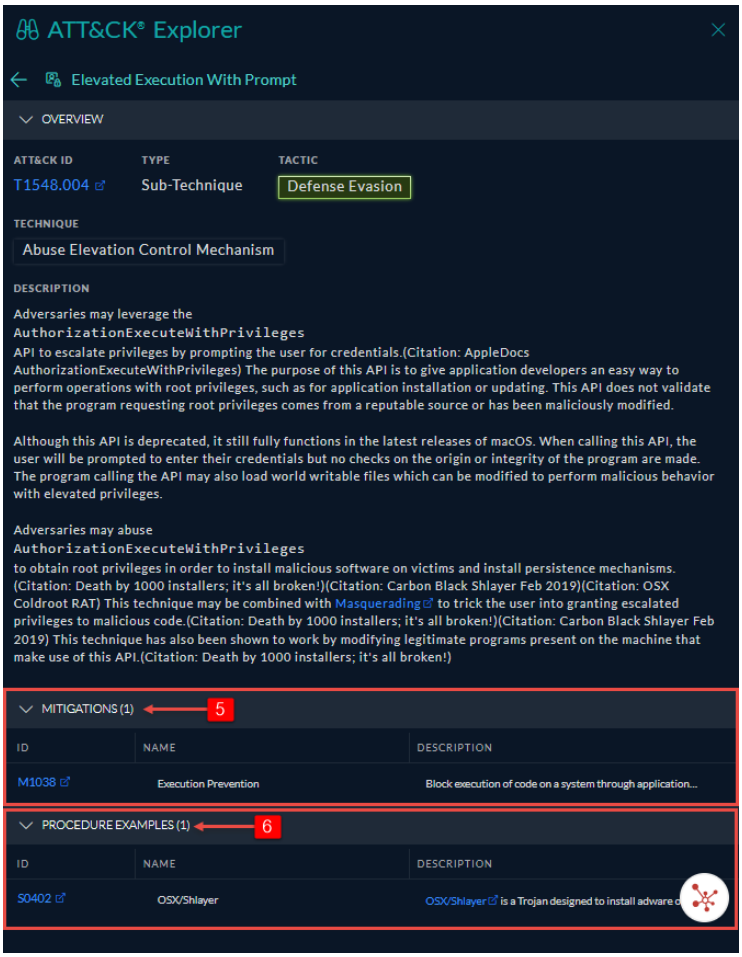
ATT&CK© Explorer Panel

ATT&CK© Explorer Panel provides information about the adversary tactics and techniques associated with the Incidents and alerts in the **Respond** view. The following table describes the various fields in the **ATT&CK© Explorer** Panel.

Fields	Description
MITRE ATT&CK Tactics	Displays the type of tactic associated with the Incident. For example: **Credential Access**. The tactic **Credential Access** tries to steal account names and passwords. For more information, see **https://attack.mitre.org/tactics/enterprise/**.
ATT&CK ID	Displays the Tactics ID associated with the Tactic. For example: **TA0006**. The Tactics ID **TA0006** is associated with the Tactic **Credential Access**.

Fields	Description
Description	Displays the detailed information about the Tactic associated with the particular incident.
Techniques	Displays the ID, Name, and the Description of the various Techniques associated with the Tactics. **Note:** Techniques are the ways with which the adversary tries to achieve a tactical goal by performing an action. For more information, see https://attack.mitre.org/resources/faq/#faq-0-0-header and https://attack.mitre.org/techniques/enterprise/.
Sub – Techniques	Displays the ID, Name, and the Description of the various Sub - Techniques associated with the Techniques. **Note:** Sub – Techniques describe the adversarial behavior at a lower level than a technique.
Mitigations	Displays the ID, Name, and the Description of the Mitigations used to prevent a technique or sub-technique from being successfully executed. For example: The Mitigation name **Account Use Policies** associated with the ID **M1036** helps configure features related to account use like login attempt lockouts and specific login times. For more information, see https://attack.mitre.org/mitigations/enterprise/.
Procedure	Examples Displays the ID, Name, and the Description of the procedures that the adversary uses for techniques or sub-techniques. For example: Lazarus Group with the ID G0032 is a North Korean state-sponsored cyber threat group that was responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. For more information, see https://attack.mitre.org/resources/faq/#faq-0-2-header and https://attack.mitre.org/groups/G0032/. **Note:** Only the first 20 Procedure Examples are displayed in the ATT&CK© Explorer panel. For more information on the other procedure examples associated with the techniques or sub - techniques, see attack.mitre.org.


ATT&CK® Explorer
Credential Access
1
OVERVIEW
2
ATT&CK ID
TYPE
TA0006
Tactic
DESCRIPTION
The adversary is trying to steal account names and passwords.
Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.
TECHNIQUES (1)
3
ID
NAME
DESCRIPTION
T1003
OS Credential Dumping
Adversaries may attempt to dump credentials to ...
SUB-TECHNIQUES (1)
4
ID
NAME
DESCRIPTION
T1003.001
LSASS Memory
Adversaries may attempt to access credential mat...


ATT&CK® Explorer
Elevated Execution With Prompt
OVERVIEW
ATT&CK ID
TYPE
TACTIC
T1548.004
Sub-Technique
Defense Evasion
TECHNIQUE
Abuse Elevation Control Mechanism
DESCRIPTION
Adversaries may leverage the
AuthorizationExecuteWithPrivileges
API to escalate privileges by prompting the user for credentials.(Citation: AppleDocs AuthorizationExecuteWithPrivileges) The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.
Although this API is deprecated, it still fully functions in the latest releases of macOS. When calling this API, the user will be prompted to enter their credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges.
Adversaries may abuse
AuthorizationExecuteWithPrivileges
to obtain root privileges in order to install malicious software on victims and install persistence mechanisms. (Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019)(Citation: OSX Coldroot RAT) This technique may be combined with Masquerading to trick the user into granting escalated privileges to malicious code.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019) This technique has also been shown to work by modifying legitimate programs present on the machine that make use of this API.(Citation: Death by 1000 installers; it's all broken!)
MITIGATIONS (1)
5
ID
NAME
DESCRIPTION
M1038
Execution Prevention
Block execution of code on a system through application...
PROCEDURE EXAMPLES (1)
6
ID
NAME
DESCRIPTION
S0402
OSX/Shlayer
OSX/Shlayer is a Trojan designed to install adware

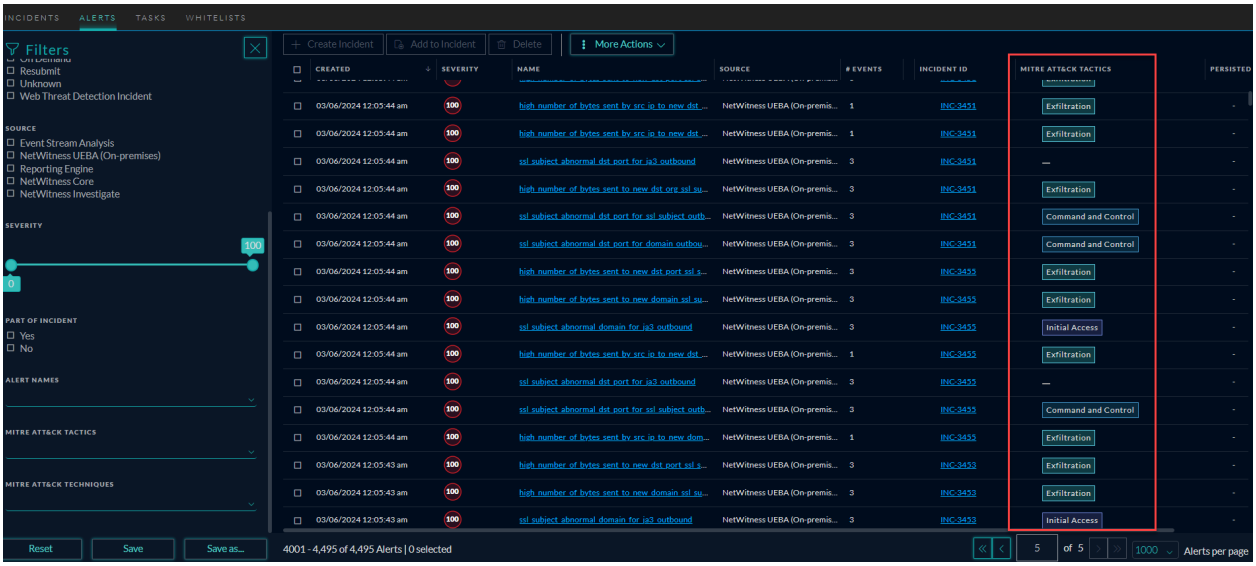
The following table explains the various sections highlighted in the above figures.

Sl.no	Description
1	This section displays the type of Tactic associated with the Incident.
2	This section displays the Tactics ID associated with the Tactic.
3	This section displays the ID, Name, and the Description of the various Techniques associated with the Tactics.
4	This section displays the ID, Name, and the Description of the various Sub - Techniques associated with the main Technique.
5	This section displays the list of the various Sub-Techniques associated with the main Technique.
6	This section displays the ID, Name, and the Description of the Mitigations used to prevent a technique or sub-technique from being successfully executed.
7	This section displays the ID, Name, and the Description of the procedures that the adversary uses for techniques or sub-techniques.

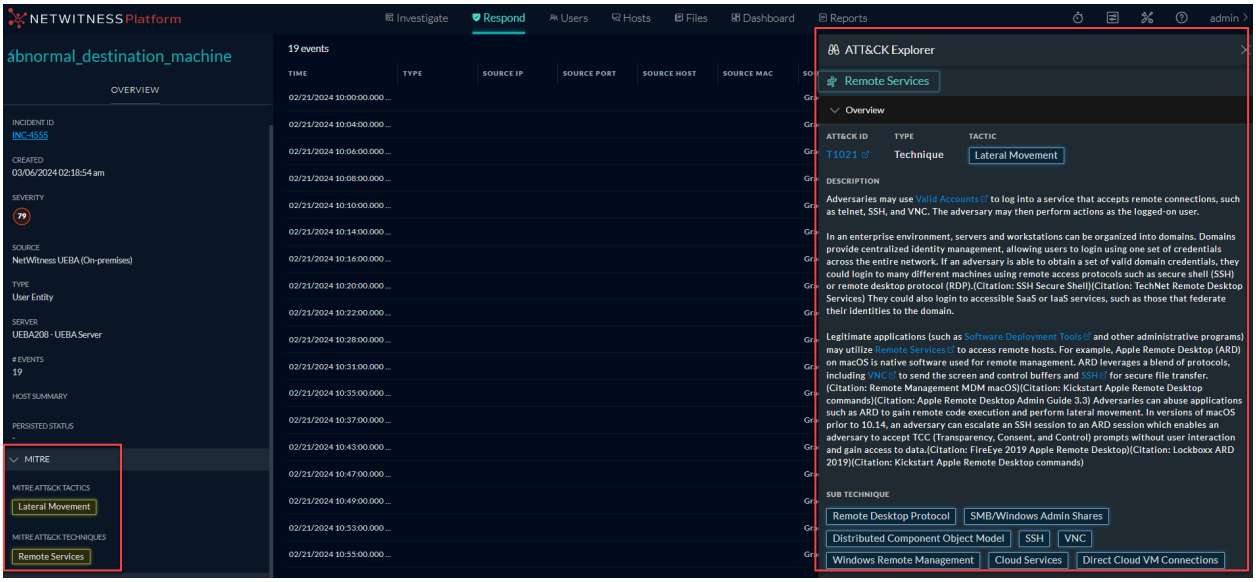
View MITRE ATT&CK Information for UEBA (On-premises)

From NetWitness Platform 12.5 or later, analysts can view the details of the tactics and techniques used by advanced attackers or advanced persistent threats (APTs) for UEBA alerts, indicators, and incidents. You do not have to search the MITRE pages to understand techniques or tactics and learn about their implications. When clicking on any tactic or technique for the UEBA alert, incident, or indicator, the ATT&CK Explorer panel will display all the details.

The following figure represents the UEBA Alert with MITRE ATT&CK Tactics column in the **Alerts** view.

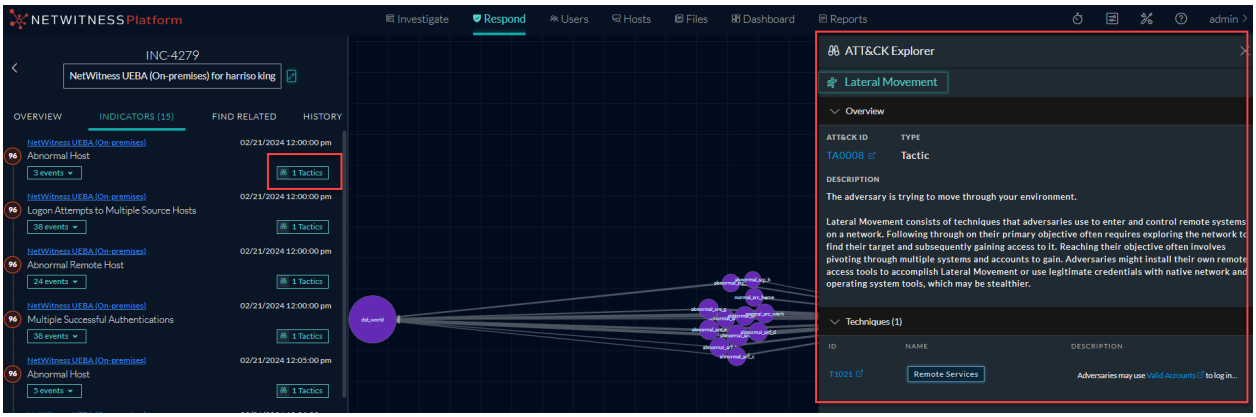


The following figure represents the UEBA Alert with Mitre ATT&CK Tactics and Techniques in the **Overview** panel of the Alert Details view.



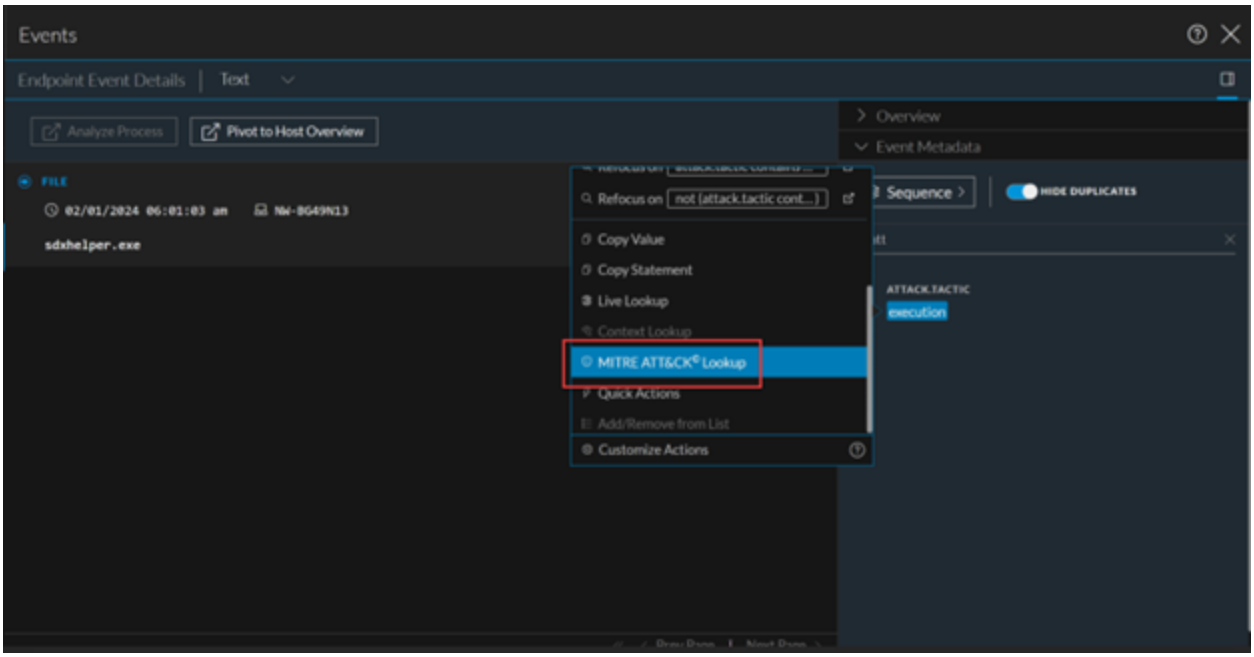
The following figure represents the UEBA Incident with MITRE ATT&CK Tactics column in the **Incidents** view.

The following figure represents the **Indicators** Panel of the Incident Details view with MITRE ATT&CK Tactics.



MITRE ATT&CK© Lookup in Respond Event Reconstruction view

In 12.4 version, the **ATTACK.TACTIC**, **ATTACK.ALL**, and **ATTACK.TECHNIQUE** meta keys in the **Event Metadata** panel or Event Reconstruction view are enhanced with **MITRE ATT&CK© Lookup** option to help analysts get more information on the MITRE Tactic and Technique associated with the particular event or the incident.



The new **ATT&CK© Explorer** Panel is displayed when you click **MITRE ATT&CK© Lookup** option.

To access MITRE ATT&CK© Lookup option

1. Go to the **Respond** view.
2. Select an Incident ID in the **Incident List** view.

The **Incident Details** view is displayed.

3. Select an event in the **Indicators** panel.

   The **Event Metadata** panel is displayed.

4. Click next to the **ATTACK.TACTIC** or **ATTACK.TECHNIQUE** meta value.
5. Select **MITRE ATT&CK© Lookup** option.

   The **ATT&CK© Explorer** Panel is displayed.

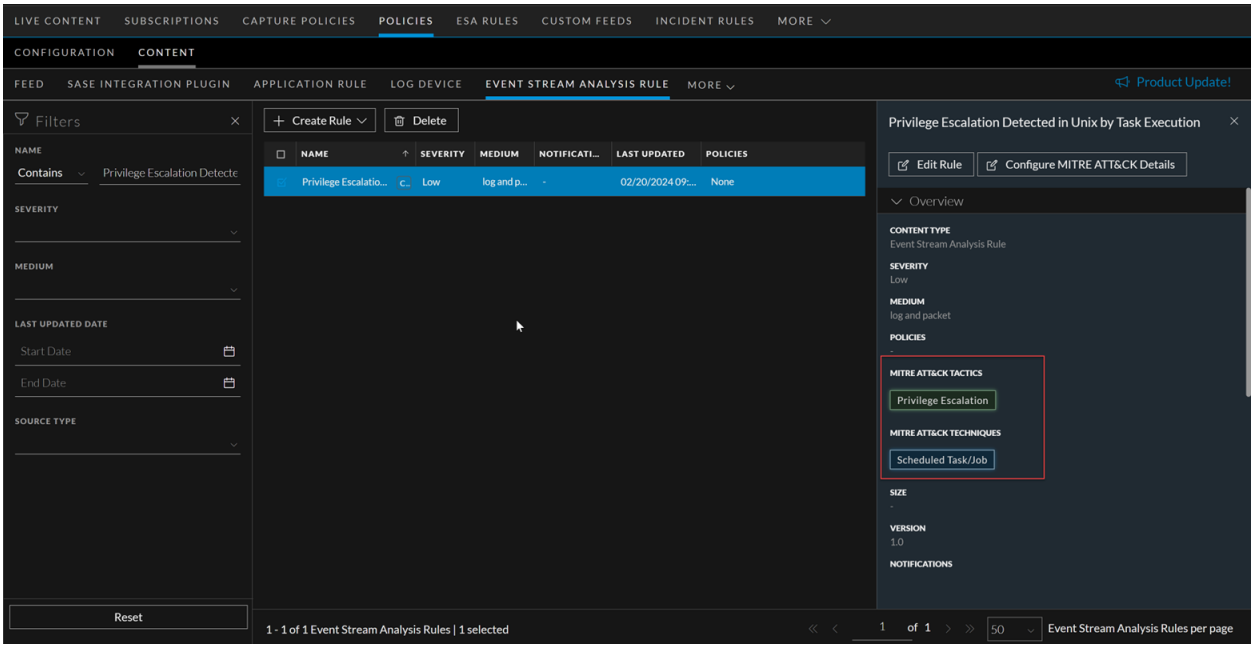
Use Case Example

The following use case provides an example of an administrator using NetWitness Platform to configure MITRE details for ESA Rules. The use case example also provides information on how an analyst can use the MITRE data configured to perform threat analysis and prevent the technique from being successfully executed.

Use Case: Configuring MITRE details for Custom ESA Rules

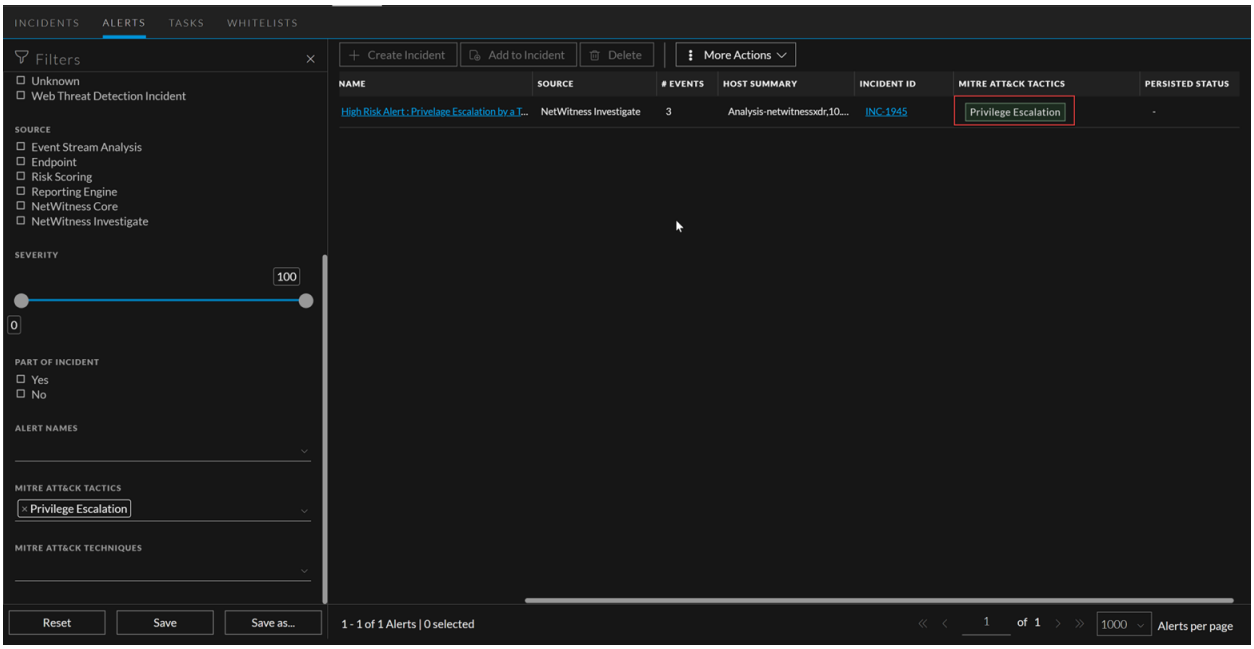
After logging in to NetWitness Platform, David, an administrator, navigates to ((**Configure**) > **Policies** > **Content** > **Content Library** > **More** > **Event Stream Analysis Rule**. Administrator selects a custom ESA rule **Privilege Escalation Detected in Unix by Task Execution** and configures the MITRE ATT&CK Tactic and MITRE ATT&CK Technique for the rule to help analyst with better insight on the threat associated with the alert or incident that is generated by this content.

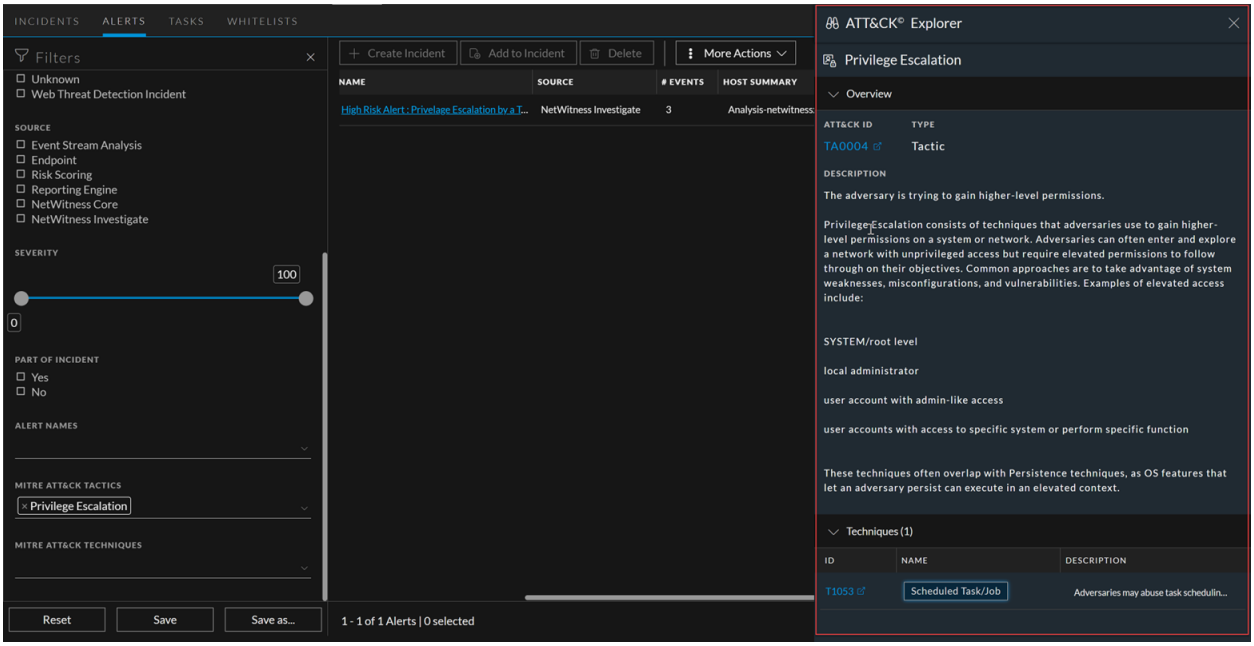
In this case, the content can identify the threat which is associated with MITRE Tactic **Privilege Escalation** and Technique **Scheduled Task/Job**. Therefore, the administrator configures **Privilege Escalation** tactic and **Scheduled Task/Job** technique to the content.



When an alert is generated with the deployed ESA content with MITRE tactic and technique configured, John, an analyst, finds this information on the Respond Alerts and Incidents.

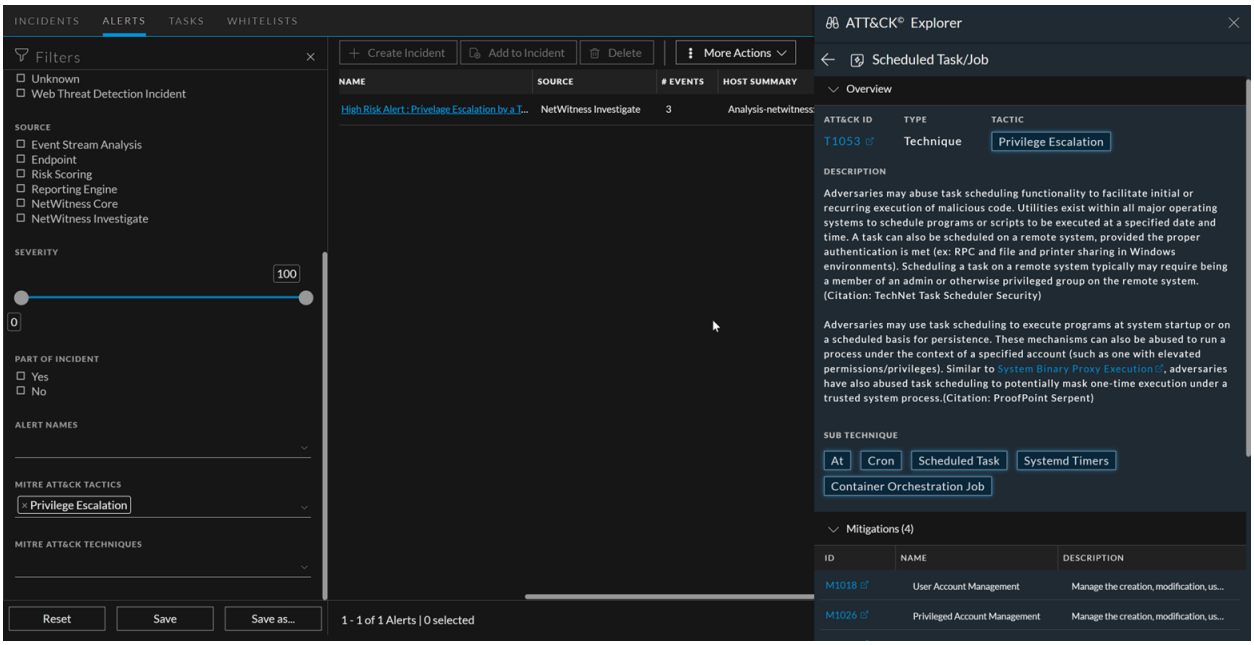
This additional MITRE context helps John to make an informed decision on responding to the incidents.

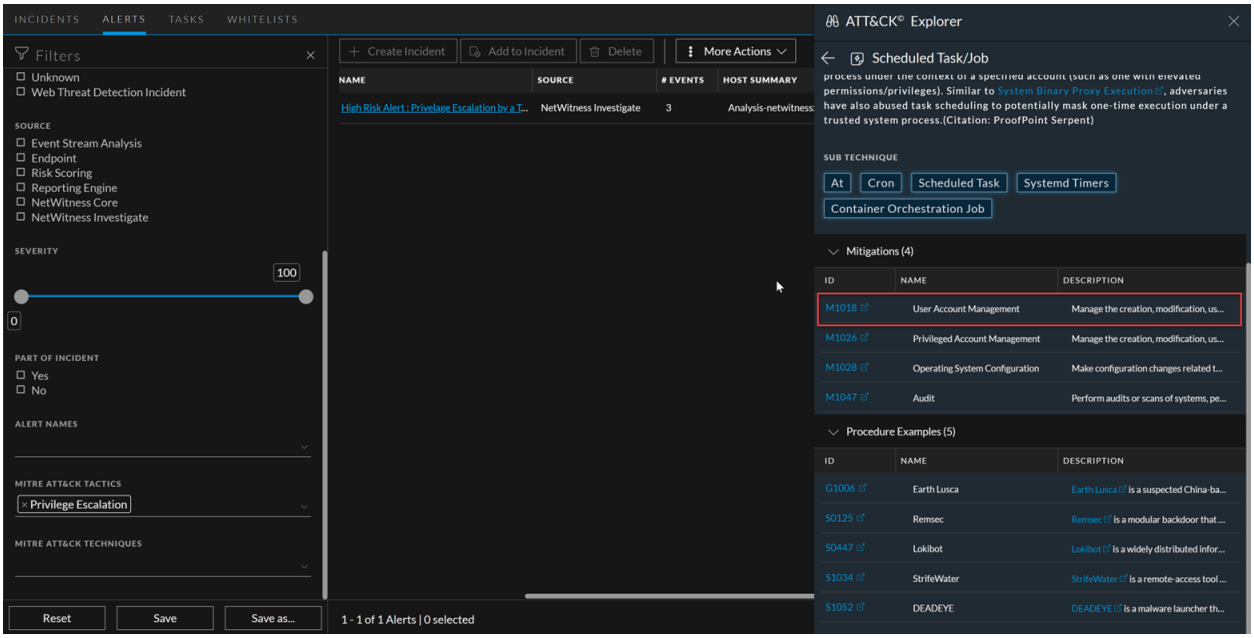




John also gets an overview on the attack tactic and technique by clicking on the MITRE tactic or technique. He further navigates over the technique, possible sub-technique, and their mitigation information.

This helps in fastening up the incident / alert triage process and take remediation steps quickly.


INCIDENTS
ALERTS
TASKS
WHITELISTS
Filters
Unknown
Web Threat Detection Incident
SOURCE
Event Stream Analysis
Endpoint
Risk Scoring
Reporting Engine
NetWitness Core
NetWitness Investigate
SEVERITY
100
0
PART OF INCIDENT
Yes
No
ALERT NAMES
MITRE ATT&CK TACTICS
Privilege Escalation
MITRE ATT&CK TECHNIQUES
Reset
Save
Save as...
Create Incident
Add to Incident
Delete
More Actions
NAME
SOURCE
EVENTS
HOST SUMMARY
High Risk Alert : Privelage Escalation by a T...
NetWitness Investigate
3
Analysis-netwitness
1 - 1 of 1 Alerts | 0 selected
ATT&CK® Explorer
Scheduled Task/Job
Overview
ATT&CK ID
TYPE
TACTIC
T1053
Technique
Privilege Escalation
DESCRIPTION
Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system. (Citation: TechNet Task Scheduler Security)
Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.(Citation: ProofPoint Serpent)
SUB TECHNIQUE
At
Cron
Scheduled Task
Systemd Timers
Container Orchestration Job
Mitigations (4)
ID
NAME
DESCRIPTION
M1018
User Account Management
Manage the creation, modification, us...
M1026
Privileged Account Management
Manage the creation, modification, us...

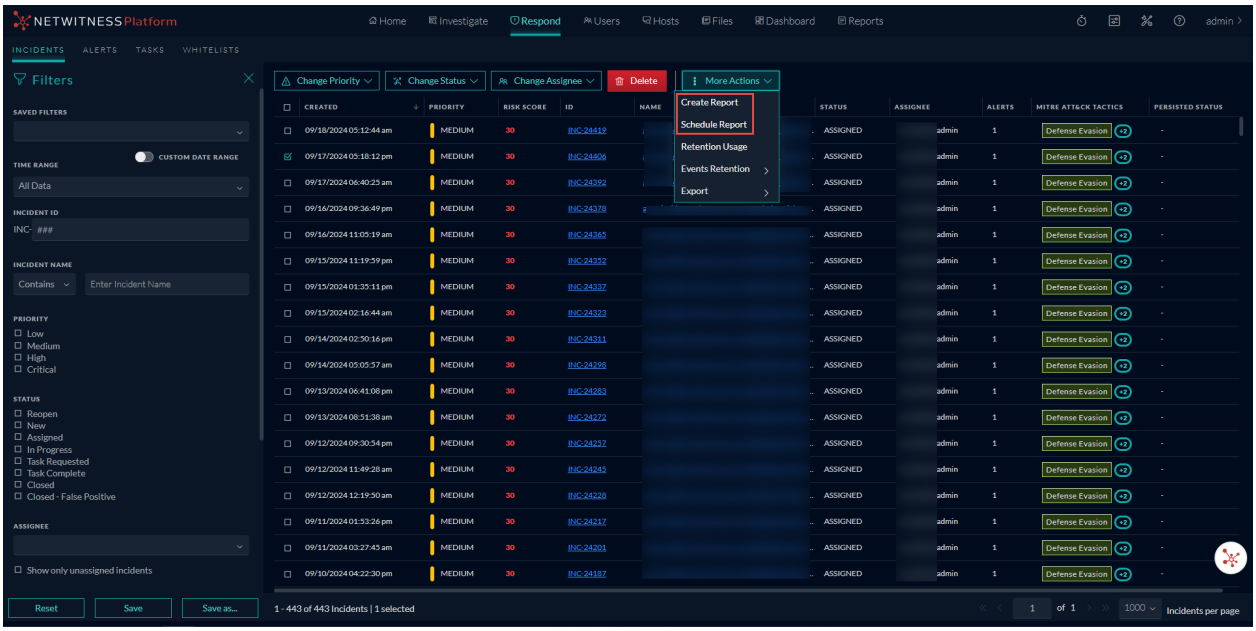

INCIDENTS
ALERTS
TASKS
WHITELISTS
Filters
Unknown
Web Threat Detection Incident
SOURCE
Event Stream Analysis
Endpoint
Risk Scoring
Reporting Engine
NetWitness Core
NetWitness Investigate
SEVERITY
100
0
PART OF INCIDENT
Yes
No
ALERT NAMES
MITRE ATT&CK TACTICS
Privilege Escalation
MITRE ATT&CK TECHNIQUES
Reset
Save
Save as...
Create Incident
Add to Incident
Delete
More Actions
NAME
SOURCE
EVENTS
HOST SUMMARY
High Risk Alert : Privelage Escalation by a T...
NetWitness Investigate
3
Analysis-netwitness
1 - 1 of 1 Alerts | 0 selected
ATT&CK® Explorer
Scheduled Task/Job
permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.(Citation: ProofPoint Serpent)
SUB TECHNIQUE
At
Cron
Scheduled Task
Systemd Timers
Container Orchestration Job
Mitigations (4)
ID
NAME
DESCRIPTION
M1018
User Account Management
Manage the creation, modification, us...
M1026
Privileged Account Management
Manage the creation, modification, us...
M1028
Operating System Configuration
Make configuration changes related t...
M1047
Audit
Perform audits or scans of systems, pe...
Procedure Examples (5)
ID
NAME
DESCRIPTION
G1006
Earth Lusca
Earth Lusca is a suspected China-ba...
S0125
Remsec
Remsec is a modular backdoor that ...
S0447
Lokibot
Lokibot is a widely distributed infor...
S1034
StrifeWater
StrifeWater is a remote-access tool ...
S1052
DEADEYE
DEADEYE is a malware launcher th...

Generate Reports from Respond View

From NetWitness Platform 12.3 or later, Users can directly create or schedule a report from the Respond view. You can create a simple ad-hoc report or complex report and configure its execution properties by scheduling a report. You can generate a report to capture details related to past, current, or predicted resource needs and schedule different time ranges to execute the same report. For example, depending on your requirement, you can schedule a report to run hourly, daily, weekly, or monthly.

Note:
- If the administrator has not configured the time zone, the reports follow the UTC time zone by default.
- If the administrator configures the time zone under the User Preferences panel, the report follows the administrator's configured time zone. For more information, see Setting User Preferences in the *NetWitness Getting Started Guide*.
- A generated output report can contain up to 100 results in tabular format.

IMPORTANT: The minimum permissions for the users required to create/schedule reports in Respond View:
- Must enable Define rule, Access configure, and Define report in the report permission section.
- Must enable alert.manage, incident.manage, alert.read, incident.read in the respond-server permission section.



- Create a Report.
- Schedule a Report.

Create a Report

The Create Report dialog enables you to create a report instantly. To create a report, you must select the incidents or alerts via their checkboxes.

Note: The report will only include data from the selected records on the screen.

To create a Report

1. Log in to the NetWitness Platform.
2. Go to **Respond** > **Incidents**.

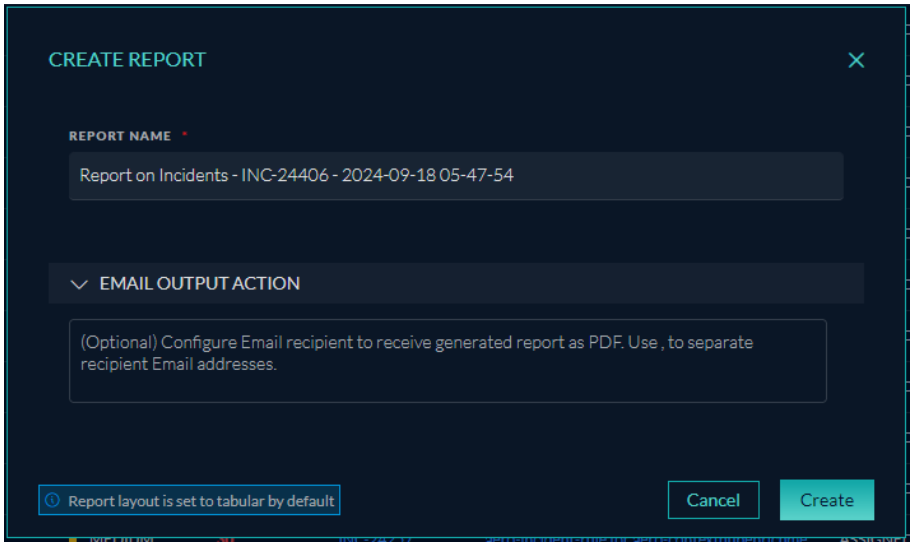
   IMPORTANT: You can create reports from the Incidents and Alerts pages separately as per your requirements. For generating reports from the Alerts page, Go to **Respond** > **Alerts**

3. Apply the required filters on the incident or alert page, select the desired records, and create a report for selected Incidents or Alerts.

   Note:
   - Once - Once the Incident or Alerts are displayed, you can sort them by ascending or descending order, and the report will be generated for the selected records.
   - To generate the reports, users must select one or more incidents or alerts.

4. Click **More Actions** > **Create Report**.

   The **Create Report** dialog is displayed.



5. The default report name with a time stamp will be displayed initially. For example, **Report on Incident - 2024-09-18 05-47-54**.

   Note:
   • You can customize the report name as per the requirement, and the name must be unique to create a report.
   • The report name must not have special characters such as / \ : * ? ” < > |.

IMPORTANT: Ensure that the SMTP mail server is configured in order to send reports to users.

6. (Optional) Click **Email Output Action** and enter the email address to which the generated report needs to be sent.

You can enter multiple comma-separated valid email IDs. For example, **email1@example.com**,**email2@example.com**,**email3@example.com**.

7. Click **Create**.

   The success message is displayed on the screen.

Note: The time required for reports to be generated may vary based on the amount of data. Please wait for the requested report to be created.

8. To view the report, do one of the following:
   - On the success message banner, click the hyperlink **click here** to directly open the report in the reports tab.
   - Go to **Reports** > **Manage** > **Reports** > **View All Reports**.

Note:
• You can download the report in a PDF or CSV file format for future and offline needs.
• When the report is generated, it is attached as a PDF to the email and sent to all users configured during the report creation process.

Schedule a Report

The Schedule Report dialog enables you to create a schedule for the report. Reports can be scheduled later (required time-line), hourly, daily, weekly, or monthly. In order to schedule a report at a specific time or on a daily, weekly, or monthly basis, you must configure the scheduling options on the Schedule tab.

Note: The report will only include data from the selected time interval. You can change the interval starting with the next recurrence.

To create a Schedule Report

1. Log in to the NetWitness Platform.
2. Go to **Respond** > **Incidents**.

   IMPORTANT: You can create reports from the Incidents and Alerts pages separately as per your requirements. For generating reports from the Alerts page, Go to **Respond** > **Alerts**

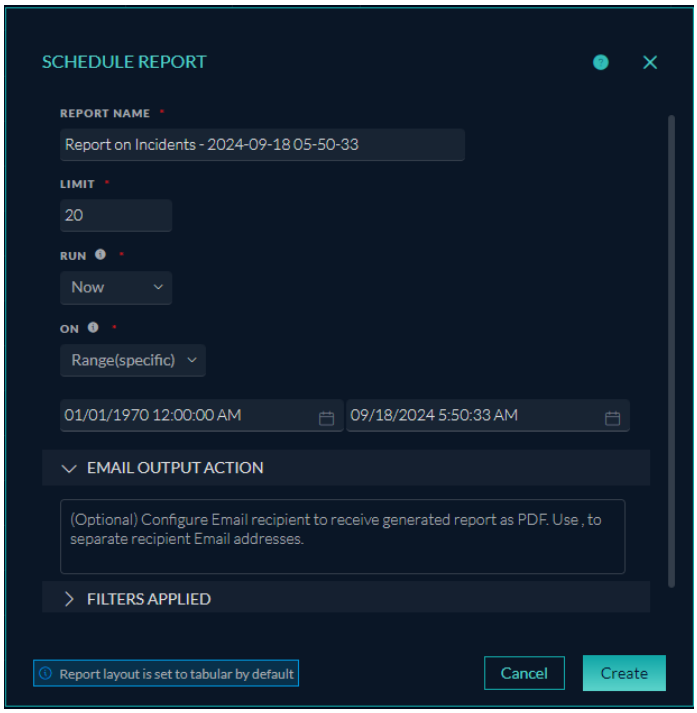
3. Apply the required filters on the incident or alert page, select the desired records, and create a report for selected Incidents or Alerts.

   All filters applied on the filters panel will be included in the reporting rule to create your report.

   Note: Once the events are displayed, you can sort the events by ascending or descending order, and the report will be generated based on the limit configured.

4. Click **More Actions** > **Schedule Report**.

   The **Schedule Report** dialog is displayed.



5. The default report name with a time stamp will be displayed initially. For example, **Report on Incident - 2024-09-18 05-50-33**.
6. Specify the following parameters to configure the Schedule.

   Depending on the type of run schedule, select one of the following:

Field	Description
Run	Time interval to use for running the scheduled job: • **Now**: If you select a Now. The system will instantly generate reports with the filters applied from the filters panel. • **Later**: If you select a **Later** run schedule, you must provide a value for the day and time in the respective field provided. • **Hourly**: If you select an **Hourly** run schedule, you must specify the minutes in the **At** Minute field. For example, if you schedule the report for 50 minutes, for every 50th minute, the report will be prepared. **Note:** A maximum of only 59 minutes can be selected. • **Daily**: If you select a **Daily** run schedule, you must enter a value in the **At** field. For example, if you schedule the report at 04:25, the report will be

Field	Description
	prepared at 04:25 AM every day. • **Weekly**: If you select a **Weekly** run schedule, you must enter a value in the **At** field and select the weekdays. **Note:** The report runs on the day of the week that the schedule begins. For example, if you schedule the report to first run on Monday, the report runs on Monday every week. • **Monthly**: If you select a **Monthly** run schedule, you must provide a value for the day and **At** field. For example, select 25 for the 25th day of the month. The report will be prepared on the 25th month of every month. **Note:** During the monthly report generation process, a message will appear if the day is greater than 28. This will notify the user that the report will be

Field	Description
	scheduled for the month containing that day.

Field	Description

ON	• **Past**: If you select the **Past** option, you can schedule the report based on **Hours**, **Days**, **Weeks**, **Months**, and **Years**. For example, if you want to schedule the report to start three days before the current date, do the following actions:
	  • Select **Past** in the **ON** field.
	  • Enter **3** in the field and select **Days** from the drop-down list.
	  This field appears only if you select **Later** in the **Run** field.
	  Note:
	  • This field appears if you select Later, Hourly, Daily, Weekly, and Monthly in the Run field.
	  • For Hourly, the maximum value allowed is 168 (24 hours x 7 days) which is counted

Field	Description
	as total hours. • **Range(specific)**: If you select Range(specific) option, you must provide the **From** and **To** values. For example, if you want to schedule the report for a specific date and time range from 02/01/2023 12:00:00 AM to 02/15/2023 12:00:00 AM. The report runs for the data on the specified period. **Note:** This field appears only if you select Later in the Run field. • **Range(generic)**: If you select **Range(generic)** option, you must provide the **From** and **To** values. For example, if you want to schedule the report daily for a time range, from 04:00 to 10:00. The report runs

Field	Description
	for the data on the specified period. **Note:** This field appears only if you select Later, Daily, Weekly, and Monthly in the Run field. **Note:** While scheduling a report, if you select the **Past** option or **Range (specific)/Range (generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.

Field	Description
Use relative time calculation	• By default, the **Use relative time calculation** option is enabled, and it uses the relative time duration to schedule a report. For example, if you schedule a report to run over the past 3 hours for the relative time, the time is exactly 3 hours from when the report is run. If the current time is 6:30 P.M., the events that occurred in the past 60 minutes or between 3:30 P.M. and 6:30 P.M. today. • You can deselect the option and schedule a report. For example, if you schedule a report to run over the past 3 hours, it will take the past 3 hours, excluding the minutes. If the current time is 6:30 P.M., the events occurred between 3 P.M. and 6 P.M. today.

IMPORTANT: Ensure that the SMTP mail server is configured in order to send reports to users.

7. (Optional) Click **Email Output Action** and enter the email address to which the generated report needs to be sent.

   You can enter multiple comma-separated valid email IDs. For example, **email1@example.com**,**email2@example.com**,**email3@example.com**.

8. Click **Create**.

   The success message is displayed on the screen.

   Note: The time required for reports to be generated may vary based on the amount of data. Please wait for the requested report to be created.

9. To view the report, do one of the following:

   - On the success message banner, click the hyperlink **click here** to navigate to the reports tab and open the generated report.
   - Go to **Reports** > **Manage** > **Reports** > **View All Reports**.

   Note:
   • You can download the report in a PDF or CSV file format for future and offline needs.
   • When the report is generated, it is attached as a PDF to the email and sent to all users configured during the report creation process.

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 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 Archer
- View All Incidents Sent to Archer
- Update an Incident
- Change Incident Status
- Change Events Retention
- Obtain Retention Usage Details
- Export Incident Data
- Export Alerts Data
- 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 Archer

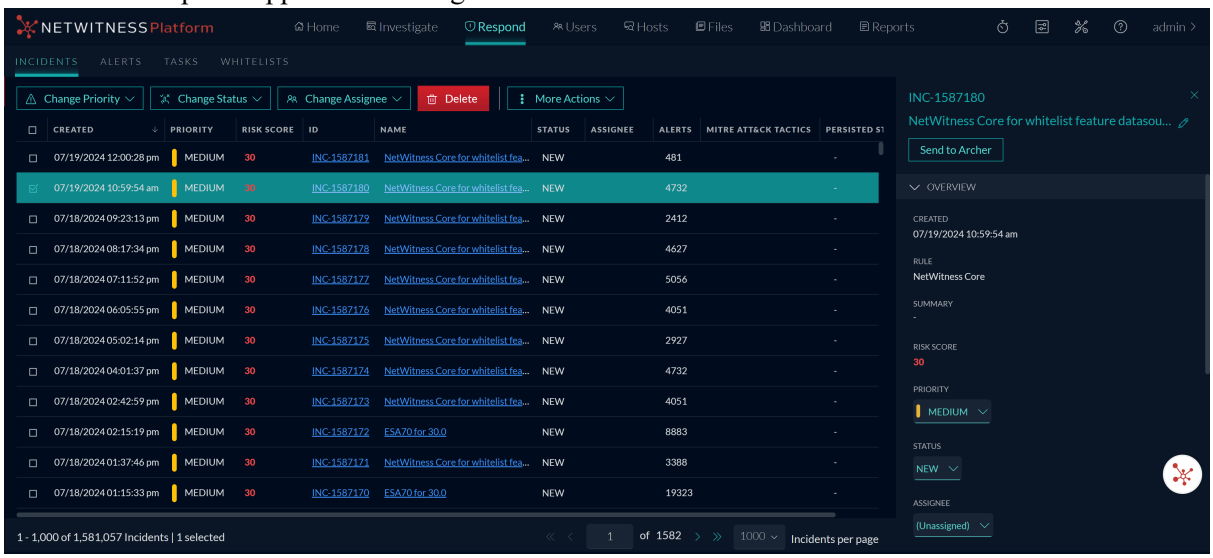
Note: This option is available in NetWitness Version 11.2 and later. If Archer is configured as a data source in Context Hub, you can send incidents to Archer and you can see the Send to Archer option and Sent to Archer Status in NetWitness Respond.

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.

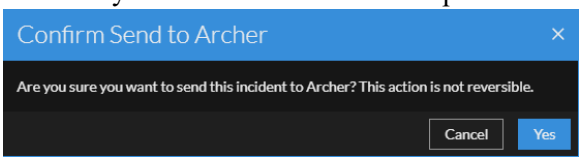
Caution: The **Send to Archer** action is not reversible.

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.

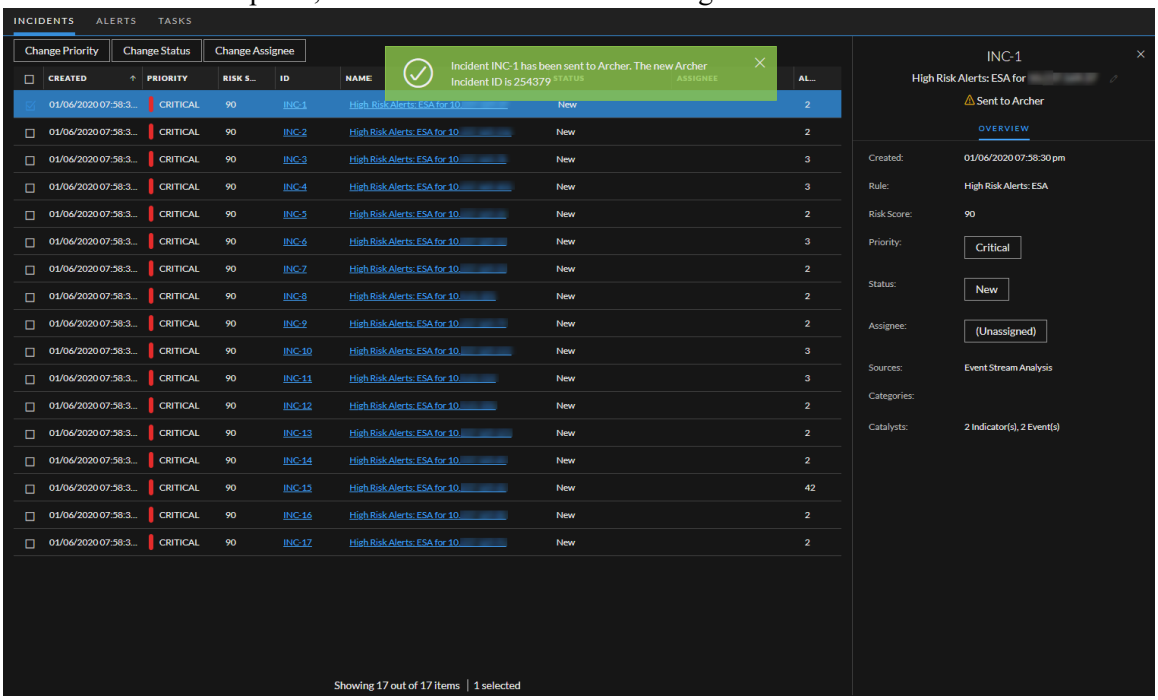


3. In the Overview panel, click **Send to Archer**.

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.



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 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.

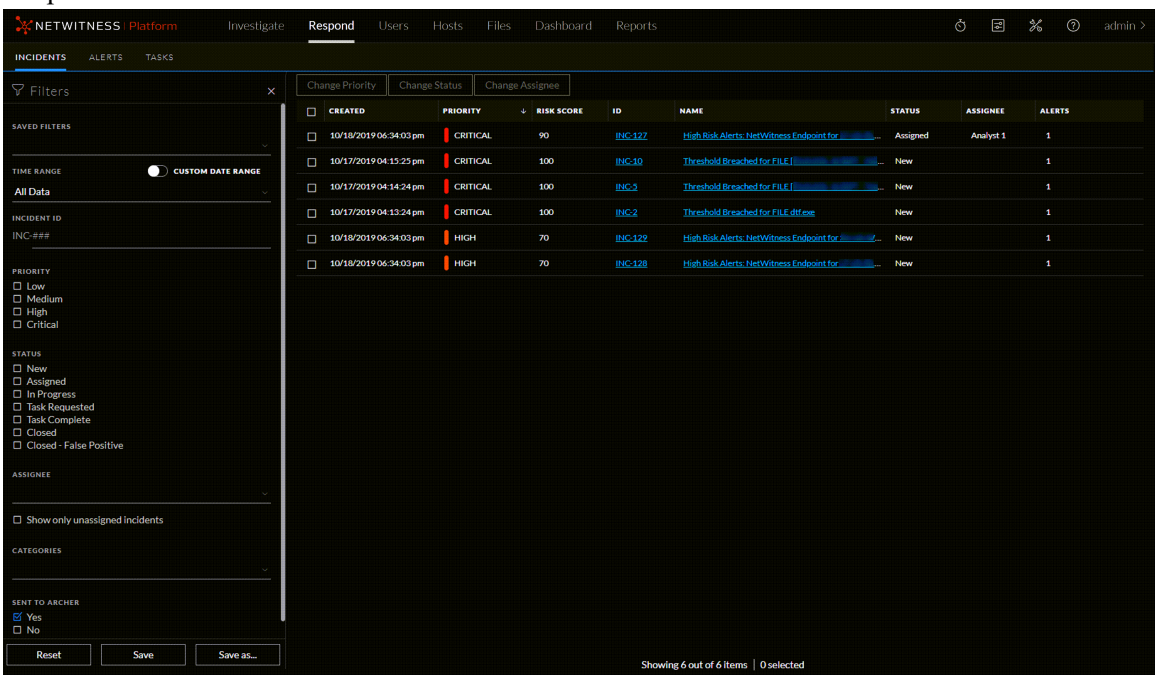
View All Incidents Sent to Archer

Note: This option is available in NetWitness Version 11.2 and later. If Archer is configured as a data source in Context Hub, you can send incidents to 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.



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:

- Reopen
- In Progress
- Task Requested
- Task Complete

- Closed
- Closed - False Positive

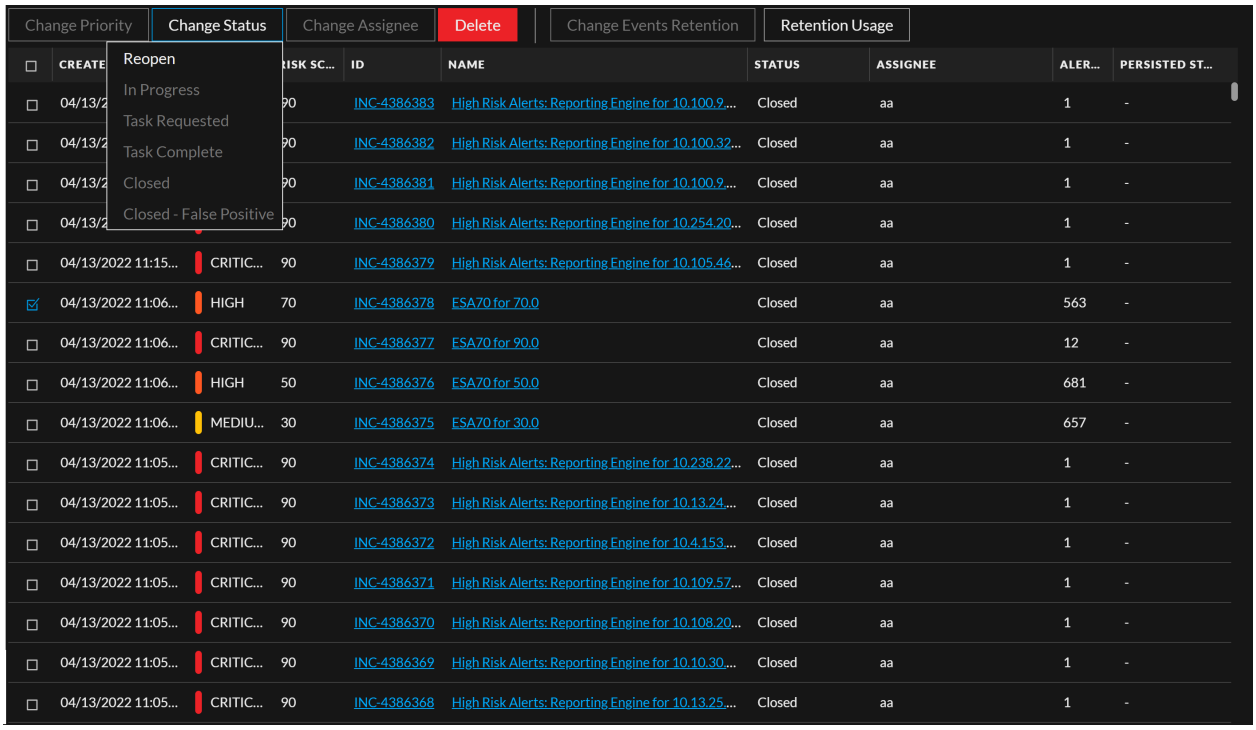
Note: New and Assigned statuses under the Change Status drop-down list are removed in the version 12.0 and later.

Status Change Workflow

The table below lists all the statuses and provides information about specific Status Change Workflow.

Status	New	Reopen	Assigned	In Progress	Task Requested	Task Complete	Closed / Closed - False Positive
New	No	No	Yes	Yes	No	No	Yes
Reopen	No	No	Yes	Yes	No	No	Yes
Assigned	No	No	No	Yes	No	No	Yes
In Progress	No	No	No	No	Yes	Yes	Yes
Task Requested	No	No	No	Yes	No	Yes	Yes
Task Complete	No	No	No	Yes	Yes	No	Yes
Closed / Closed - False Positive	No	Yes	No	No	No	No	No

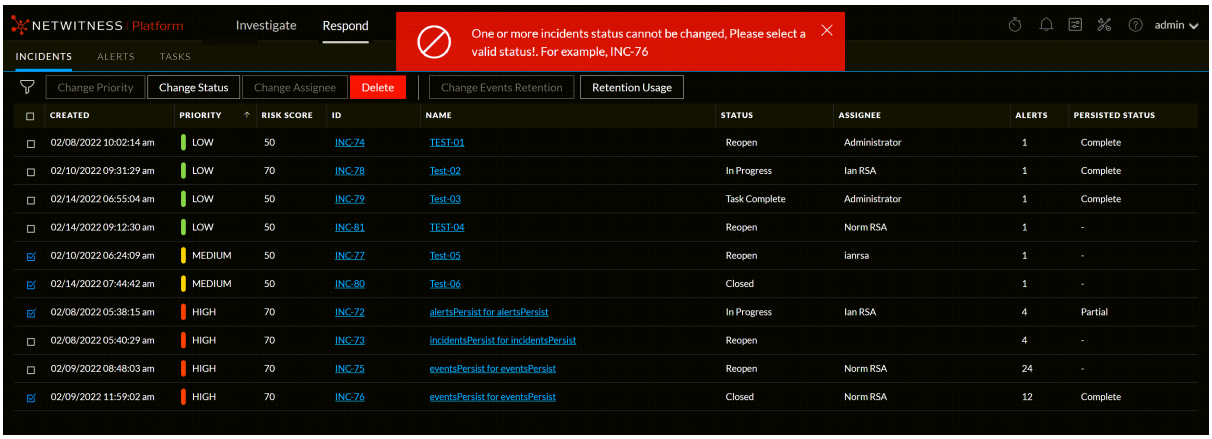
Note: When you select an incident and click Change Status, all the invalid statuses are grayed out under the Change Status drop-down list. This is not applicable for multi-select of incidents. Refer the following figure.



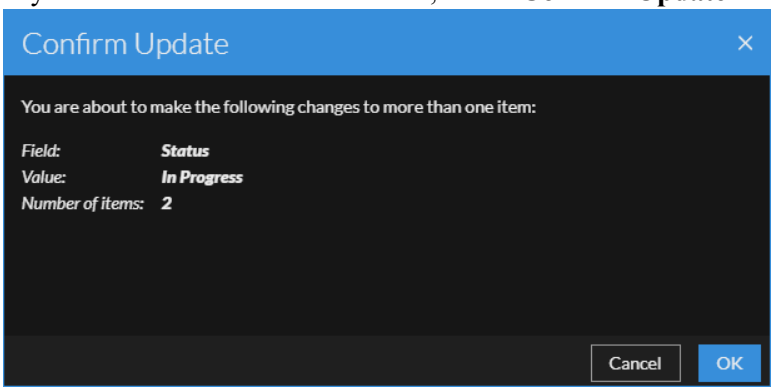
To update the status of multiple incidents:

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 Assignee would like to change it to In Progress for the selected incidents.

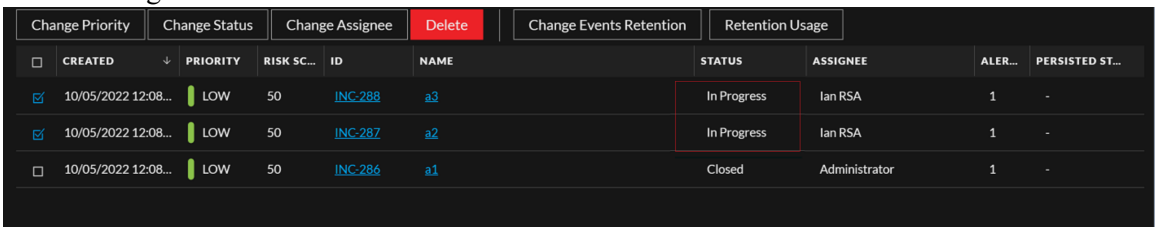
Note: The incident status can be changed to **Reopen** only if the current status of the incident is **Closed** or **Closed - False Positive**. This is also applicable when multiple incidents are selected. Even if one of the multiple incidents selected has the status other than **Closed or Closed - False Positive**, the error message **One or more incidents status cannot be changed, Please select a valid status!. For example, INC-x** is displayed. Refer the following figure.



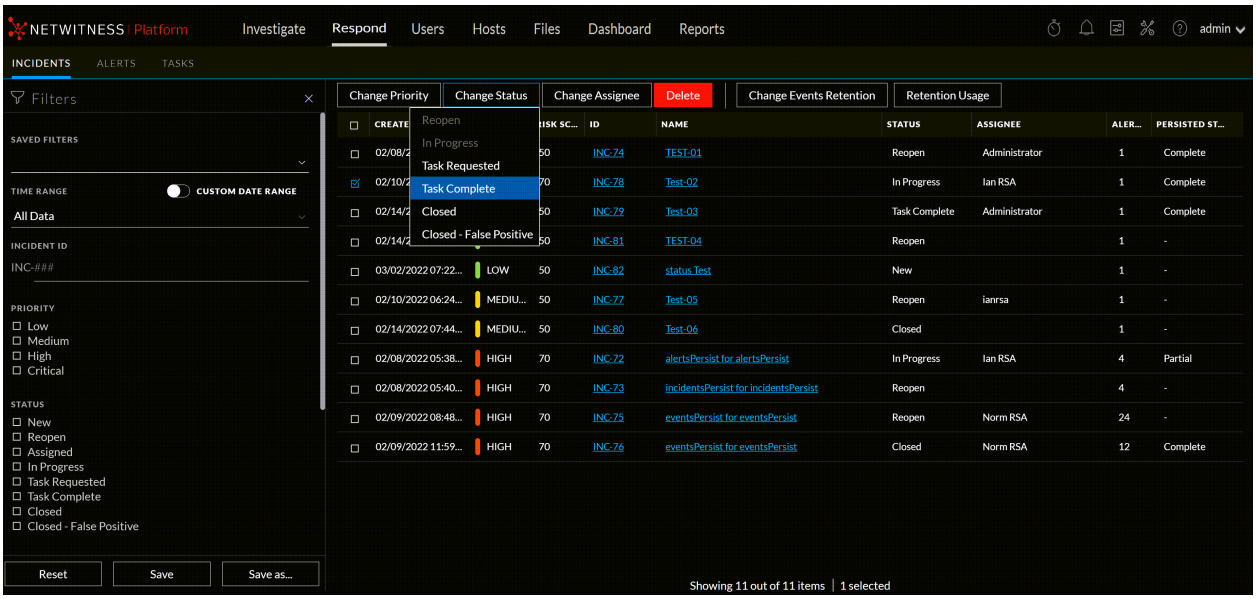
3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.



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

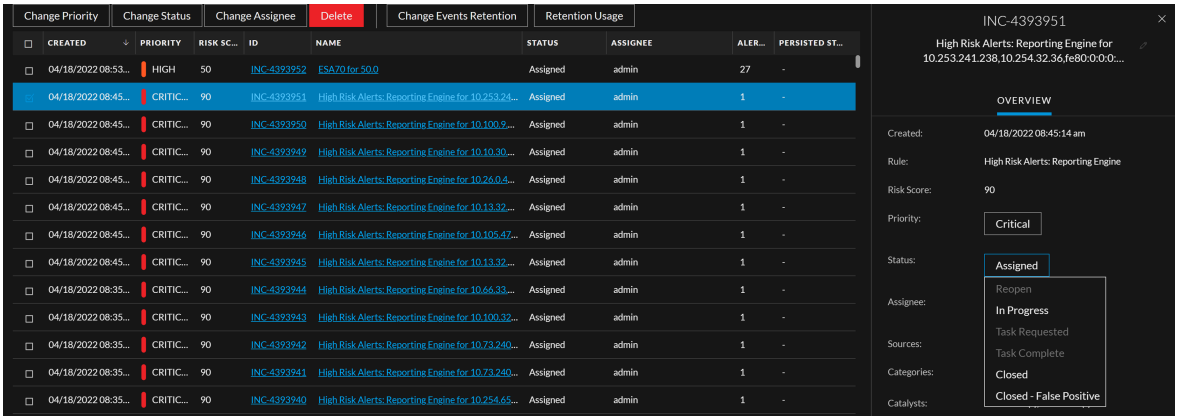


Note: If you select any incident and click **Change Status**, the current status of the incident is grayed out in the drop-down list. This is not applicable if you select multiple incidents. Refer the following figure.

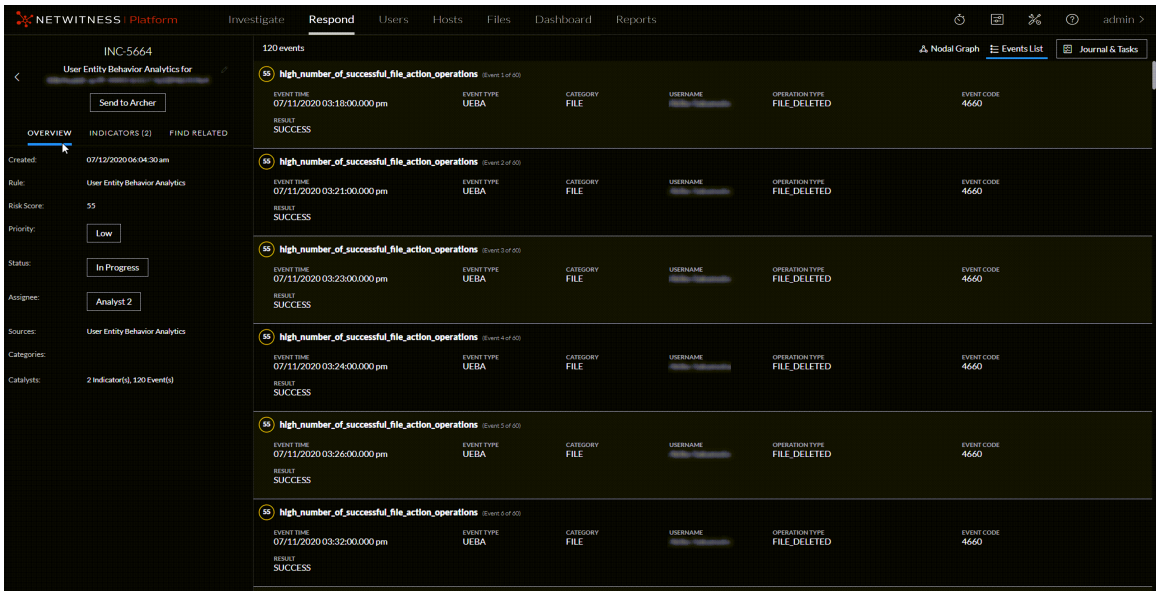


To change the status of a single incident from the Overview panel:

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

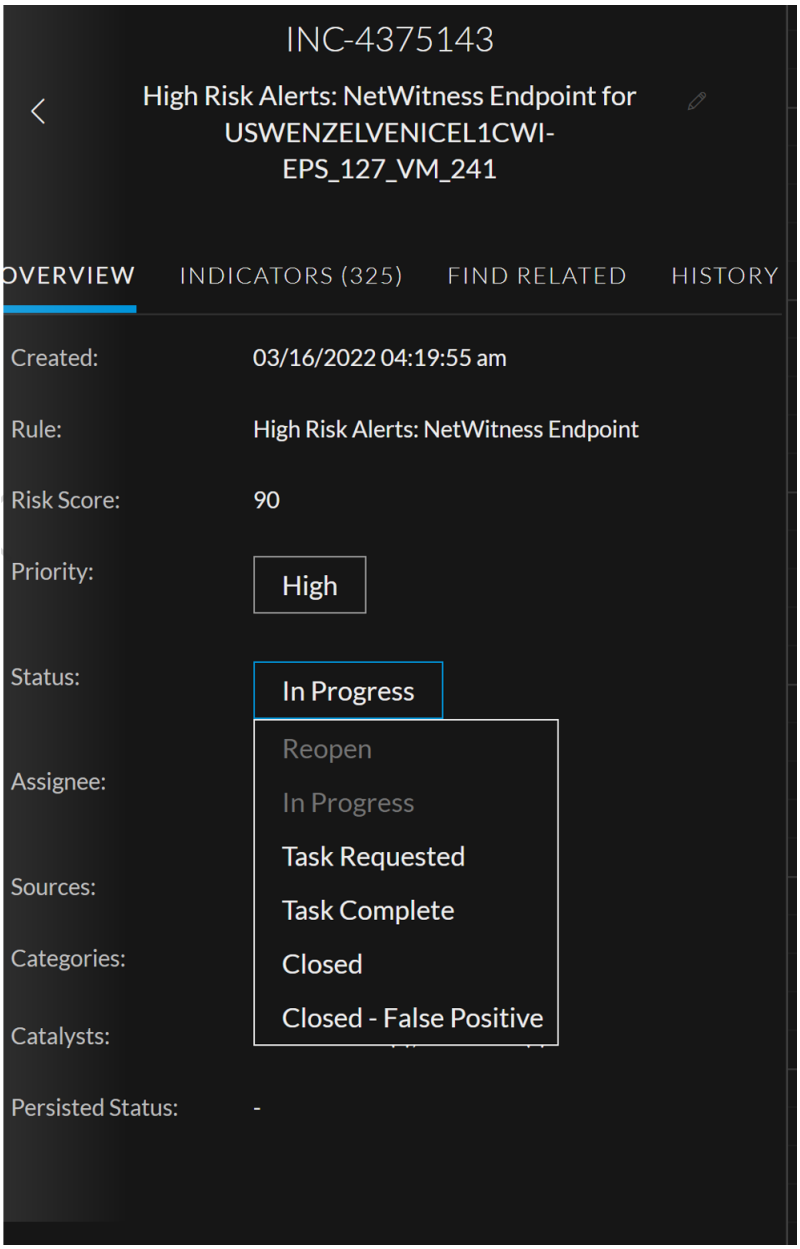


- From the Incident Details view, click the **OVERVIEW** tab.

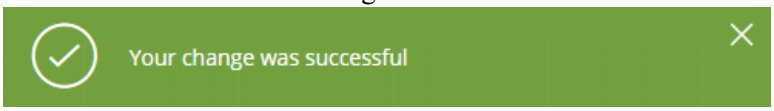


In the Overview panel, the Status button shows the current status of the incident.

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



You can see a successful change notification.



Note: The incident status can be changed to **Reopen** only if the current status of the incident is **Closed** or **Closed - False Positive**.

Change Events Retention

Events retention enables you to persist events that are associated with particular incidents, thereby enabling you to view the incident related events in the future, regardless of its age. The event data will always be available for viewing and reconstruction as long as the event is persisted, enabling you to easily refer back to details, even if the original event has rolled over from the NetWitness database. You can perform the following functions:

- Persist all events
- Suspend persisting all events

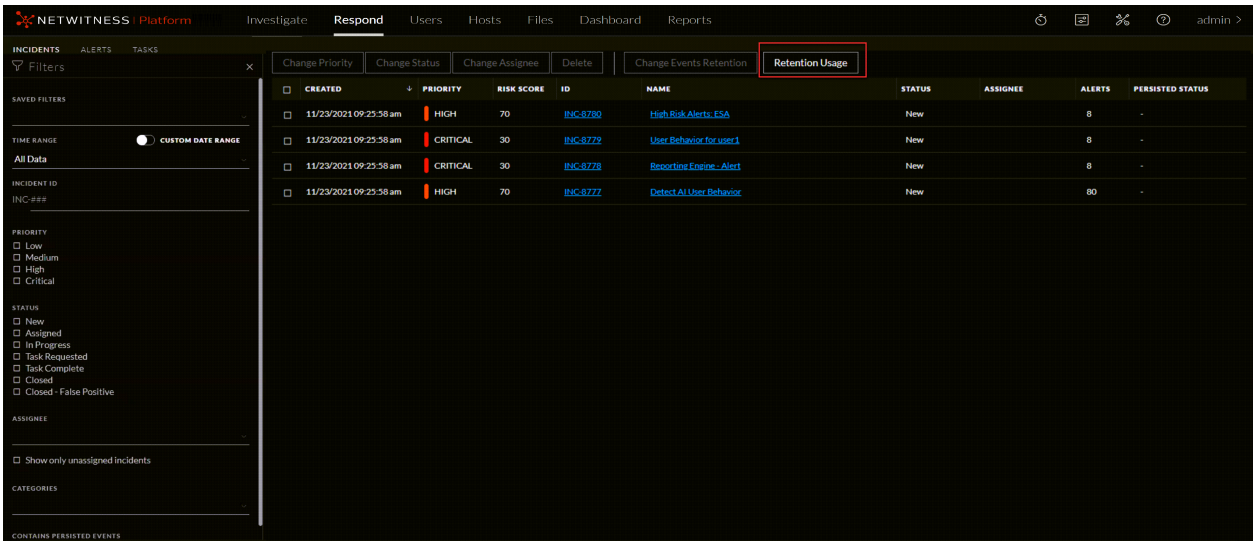
To change event retention:

1. Select the incidents for which you want to change the event retention plan.
2. Select **Persist all events** from the **Change Events Retention** tab to persist all the events that are associated with the selected incidents.
   a. The confirmation message appears. Click **OK** to persist all events.
   Persisting all events in an incident in NetWitness will save the events data in the long term cache of the source.
3. Select **Suspend Persisting all events** from the **Change Events Retention** tab to stop persisting the events that are associated with the selected incidents.
   a. The confirmation message appears. Click OK to suspend persist all events.
   Suspending persist of events in an incident from NetWitness will delete it from the long term cache of the source only. This may not be reversible if the original event data has rolled out in the source database.

Note: You cannot change the event retention for incidents that are in **New** or **Closed** state.

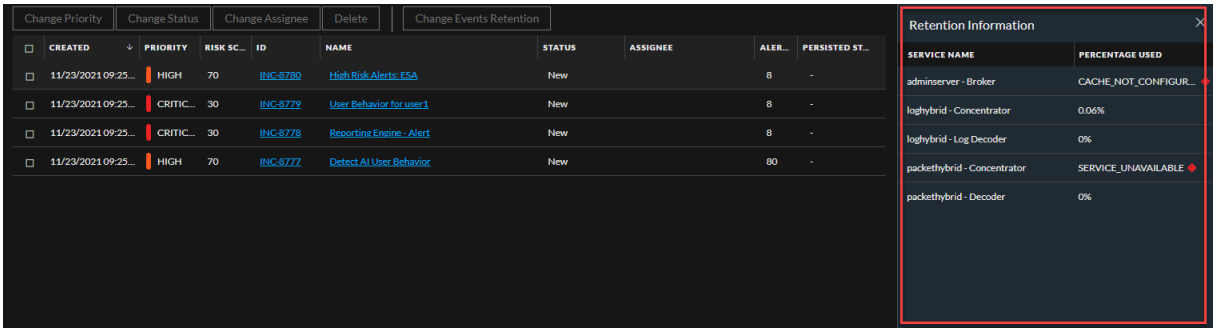
Obtain Retention Usage Details

The Retention Usage tab allows an analyst to fetch all the persisted data disc usage stats of all the configured services and the percentage used by the pinned cache directories. This will enable the analyst to determine if the disk is running out of space and if additional space needs to be added or suspend persist on the existing events in an incident.



After the analyst clicks on the Retention Usage tab, a Retention Information panel is displayed with the following status:

- Percentage of the disk used when data is persisted
- Cache directory is configured or not. In case it is not configured it is explicitly indicated.
- List of all the status of a configured service. In case the service is not available it is explicitly indicated.



Note: In case the disk space exceeds the usage, a warning message displayed. The service threshold can be configured by navigating to **Respond** > **Services** > **respond/core/properties** > **warning-threshold field**.

Export Incident Data

NetWitness Platform enables the analysts to export and store the Incidents with Alerts and Events in JSON format for offline investigation. The **Export** drop-down allows you to export and download the data (such as fields or attributes) associated with Alerts and Events of the selected Incidents. The data can only be downloaded in JSON format.

Schema Files for Incident Export

NetWitness Platform provides Schema files (Default and Custom) located at `/var/netwitness/respond-server/export-schema` to allow you to export only a subset of attributes among the many list of attributes available in Mongo DB for Incidents and Alerts. Default schema files cannot be modified, but the Custom schema files can be modified to add the attributes as required. For more information, see Schema Files for Incidents and Schema Files for Alerts.

Schema Files for Incidents

The Incident Schema files contain various fields or attributes associated with an Incident. Based on the requirement, you can modify these Schema files and download additional fields. The Schema files are categorized into two types:

- **Default Incident Schema File** (**default_incident_export.json**): This file contains a default list of attributes associated with the Incidents (in Mongo DB) that are used to export. This pre-populated out-of-the-box file provided by NetWitness Platform must not be modified.
- **Custom Incident Schema File** (**custom_incident_export.json**): This is an empty file provided by NetWitness Platform to allow users to download the attributes unavailable in the **Default Incident Schema File**, but listed in the **incident** collection in Mongo DB.

  To download the required attributes using Custom Incident Schema File:

  1. Edit the `custom_incident_export.json` file located at `/var/netwitness/respond-server/export-schema` to add the required attributes.
  2. Restart the **Respond** Service.
  3. Export the Incidents data from UI.

  Note: The attributes downloaded using the **Custom Incident Schema File** include the attributes already listed in the **Default Incident Schema File** and the newly added attributes.

Schema Files for Alerts

NetWitness Platform allows you to download various fields or attributes associated with the Original and Normalized alerts.

Original Alerts

The alerts triggered and received through different sources such as Endpoint, NetWitness UEBA (On-premises), Event Stream Analysis (ESA), Malware Analysis, NetWitness Investigate, Reporting Engine, Risk Scoring, Web Threat Detection, NetWitness UEBA (Cloud), and NetWitness Insight are Original Alerts.

Normalized Alerts

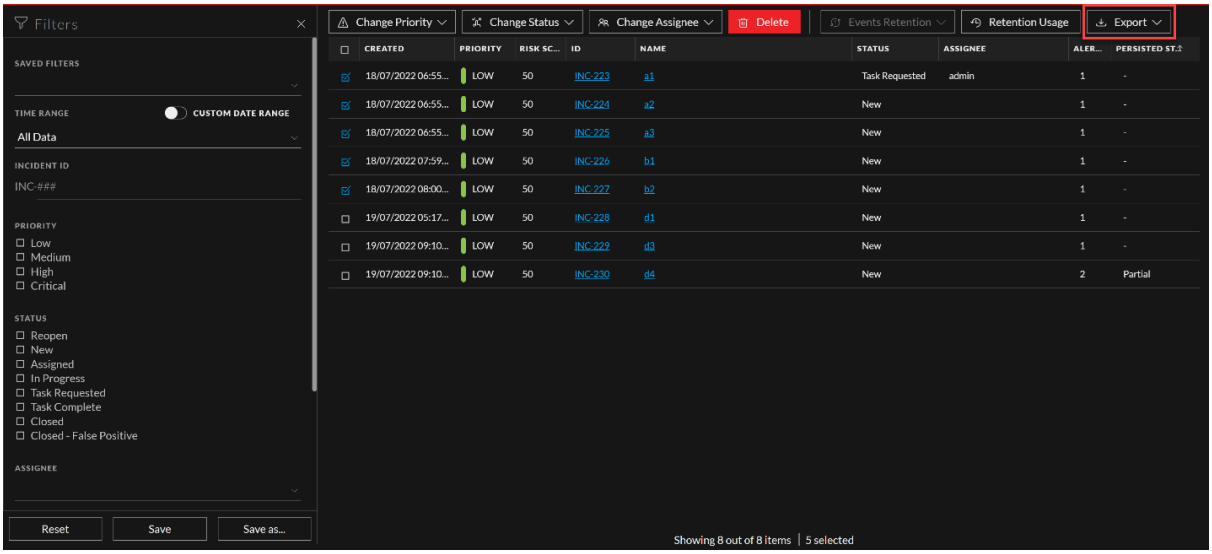
The structure or pattern of the Original Alerts varies based on the source from which the alerts are triggered. These alerts are normalized and standardized in the **Respond** service to unify their structure.

Based on the attributes (associated with the Original and Normalized Alerts) downloaded, the Alerts Schema files are categorized into:

- **Default Original Alerts Schema File** (**default_alert_original_export.json**): This file contains a default list of attributes associated with the Original Alerts (in Mongo DB) that are used to export. This pre-populated out-of-the-box file provided by NetWitness Platform must not be modified.
- **Custom Original Alerts Schema File** (**custom_alert_original_export.json**): This is an empty file provided by NetWitness Platform to allow you to download the attributes unavailable in the **Default Original Alerts Schema File**, but listed in the **originalAlert** (**alert** > **originalAlert**) collection in Mongo DB.
- **Default Normalized Alerts Schema File** (**default_alert_normalized_export.json**): This file contains a default list of attributes associated with the Normalized Alerts (in Mongo DB) that are used to export. This pre-populated out-of-the-box file provided by NetWitness Platform must not be modified.
- **Custom Normalized Alerts Schema File** (**custom_alert_normalized_export.json**): This is an empty file provided by NetWitness Platform to allow you to download the attributes unavailable in the **Default Normalized Alerts Schema File**, but listed in the **alert** (**alert** > **alert**) collection in Mongo DB.

To export the Incident data:

1. Go to **Respond** > **Incidents**.
2. In the Incidents List view, select one or more incident and click the **Export** drop-down.



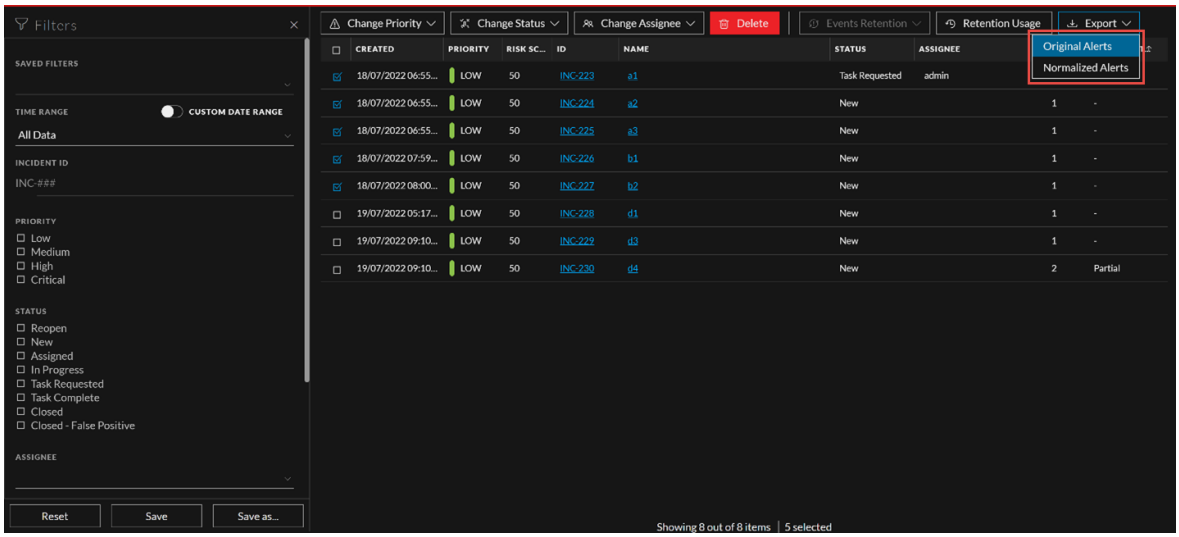
IMPORTANT: To access the **Export** drop-down, you must have access to escalate or remediate the incident.

Note: The **Export** drop-down is enabled only in the following scenarios:
- When an incident is selected in the Incidents List view.
- When the different set of incidents are selected in the Incidents List view after incident data export.
- When you select the same set of incidents again in the Incidents List view to export the data.

Note:
- You must refresh the page to select the same set of incidents again in the Incidents List view to export the data.
- You can export data of a maximum of ten incidents at a time. Once the data download is in progress, you can select a different set of incidents (ten incidents) and export their data simultaneously. You can repeat this action until the condition **max-user-tasks** (a maximum limit set for exporting the incidents data in the **Respond** service under **rsa.respond.incident.exports**) is met.

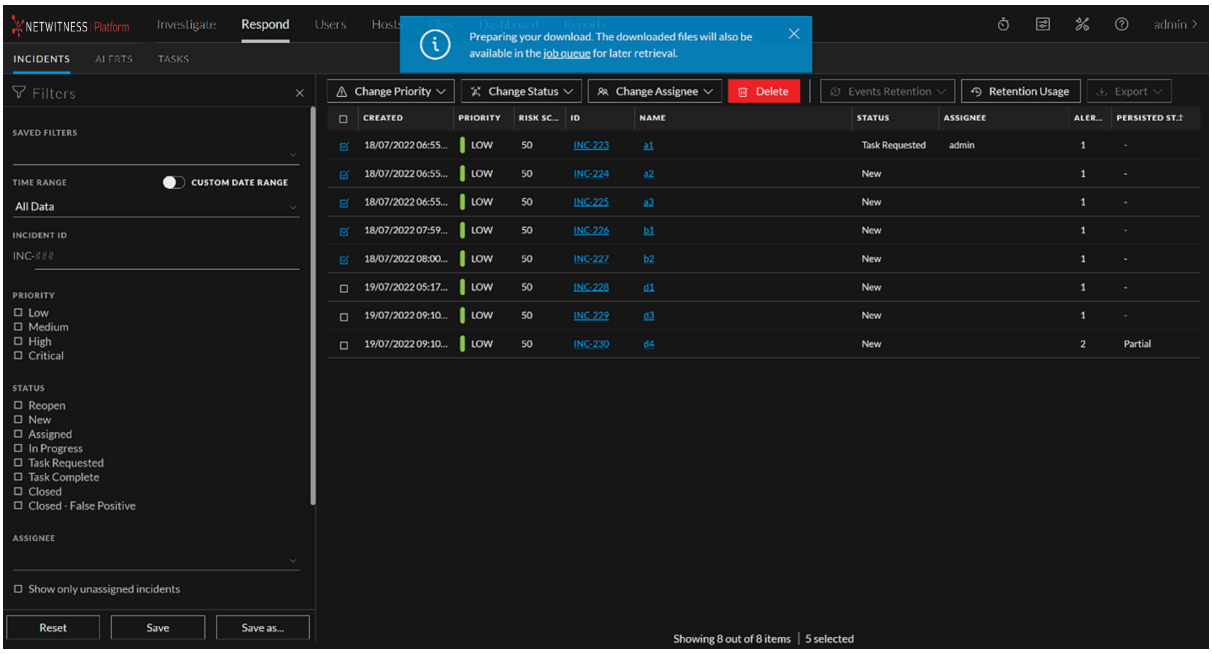
3. Select one of the following options in the **Export** drop-down list to download the files.

   - **Original Alerts**: Select this option to download the attributes associated with the Original Alerts. For more information, see Original Alerts.
   - **Normalized Alerts**: Select this option to download the attributes associated with the Normalized Alerts. For more information, see Normalized Alerts.



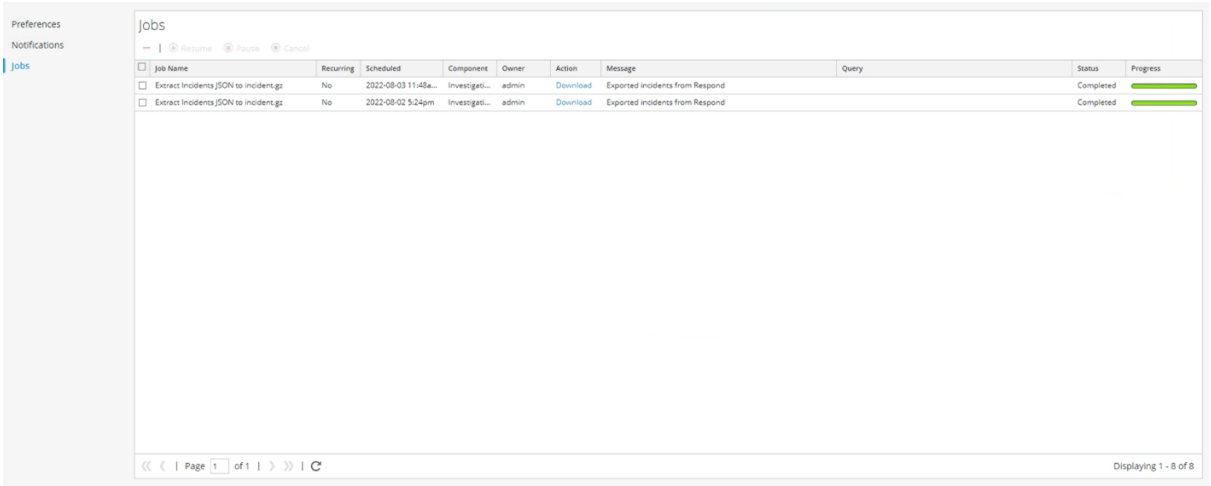
   Once the file download is initiated, a notification message is displayed.

4. Click the **job queue** link.



The **Jobs** page is displayed.

5. Select the file and click **Download** under the **Action** column once the download status is displayed as **Completed** under the **Status** column.



Export Alerts Data

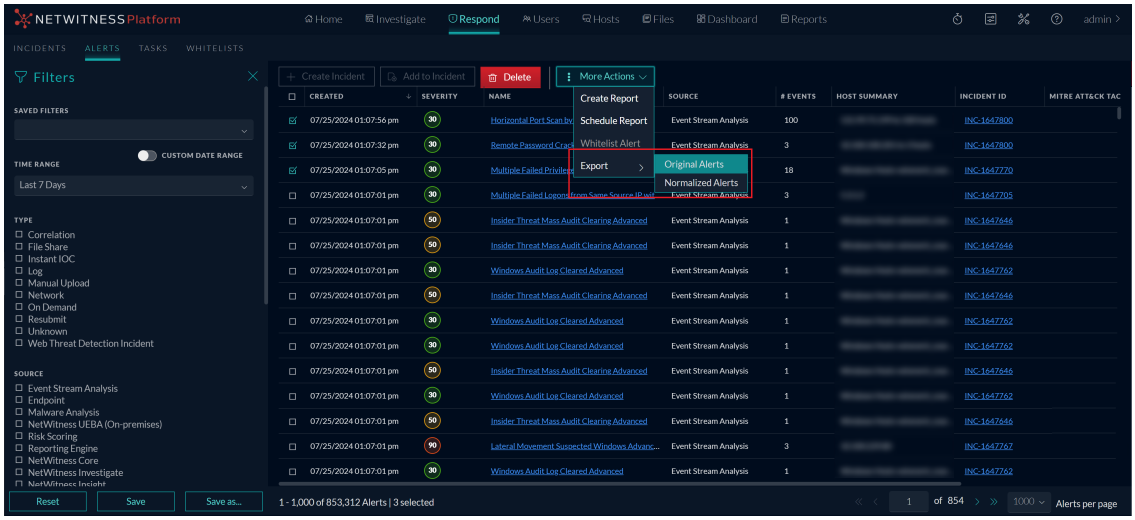
NetWitness Platform allows you to export up to 1000 alerts at a time in the JSON format for offline investigation. The **Export** option in **Respond** > **Alerts** > Select an alert > **More Actions** allows you to export and download the original and normalized alerts along with the events.

Schema Files for Alert Export

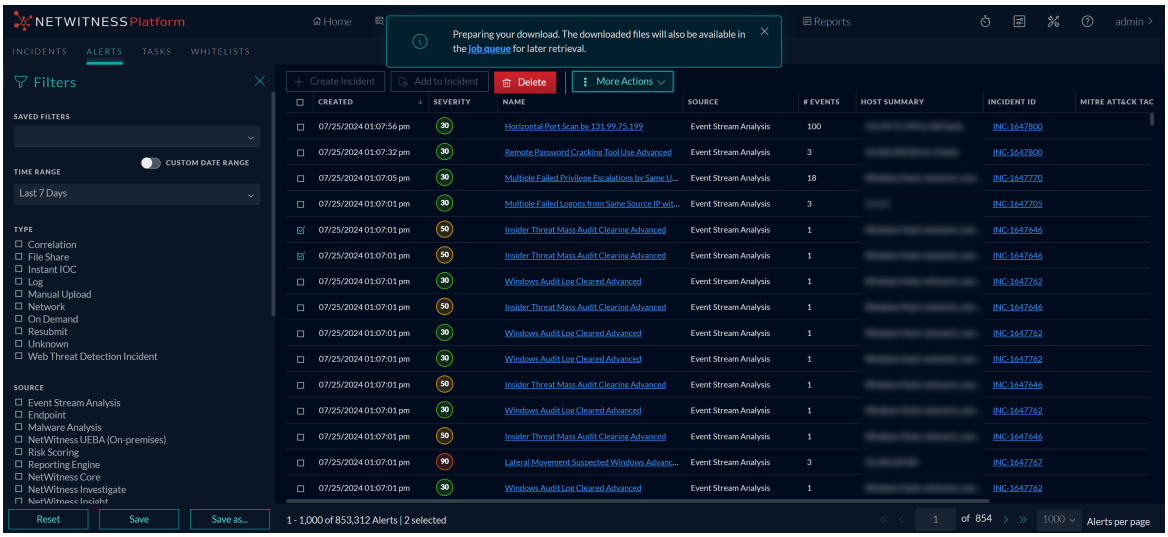
NetWitness Platform provides Schema files (Default and Custom) located at `/var/netwitness/respond-server/export-schema` to allow you to export only a subset of attributes among the many list of attributes available in Mongo DB for Alerts. Default schema files cannot be modified, but the Custom schema files can be modified to add the attributes as required. For more information, see Schema Files for Alerts.

To export the Alerts data

1. Go to **Respond** > **Alerts**.
2. In the Alerts List view, select one or more alerts.
3. Go to **More Actions** > **Export** and select one of the following types of Alert to be exported.
   - **Original Alerts**: Select this option to export the Original Alerts and their event data. For more information on the Original Alerts, see Original Alerts.
   - **Normalized Alerts**: Select this option to export the Normalized Alerts and their event data. For more information on the Normalized Alerts, see Normalized Alerts.

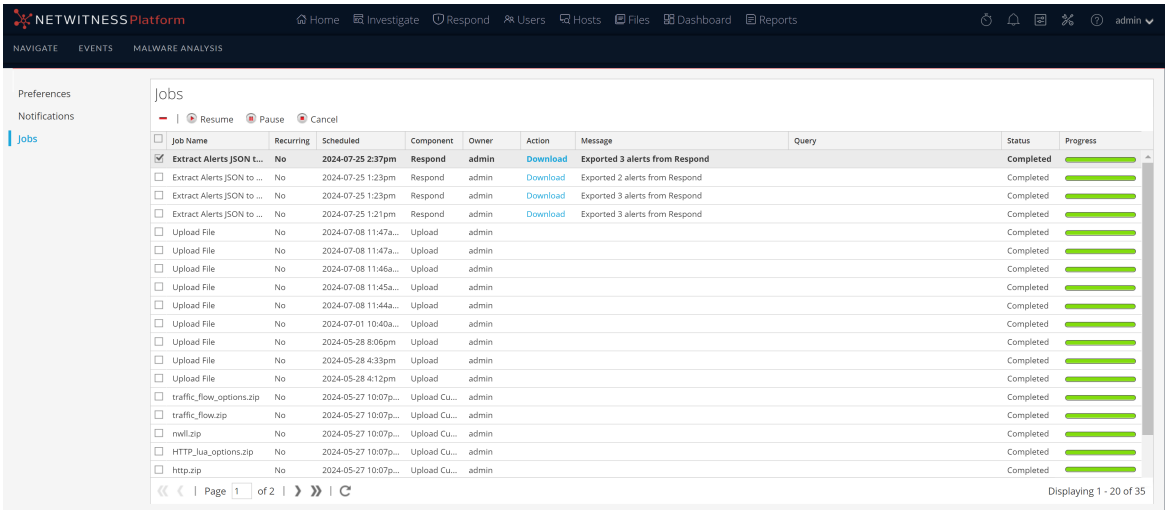


4. Click the **job queue** link.



The **Jobs** page is displayed.

5. Select the file and click **Download** under the **Action** column once the download status is displayed as **Completed** under the **Status** column.



Change Incident Priority

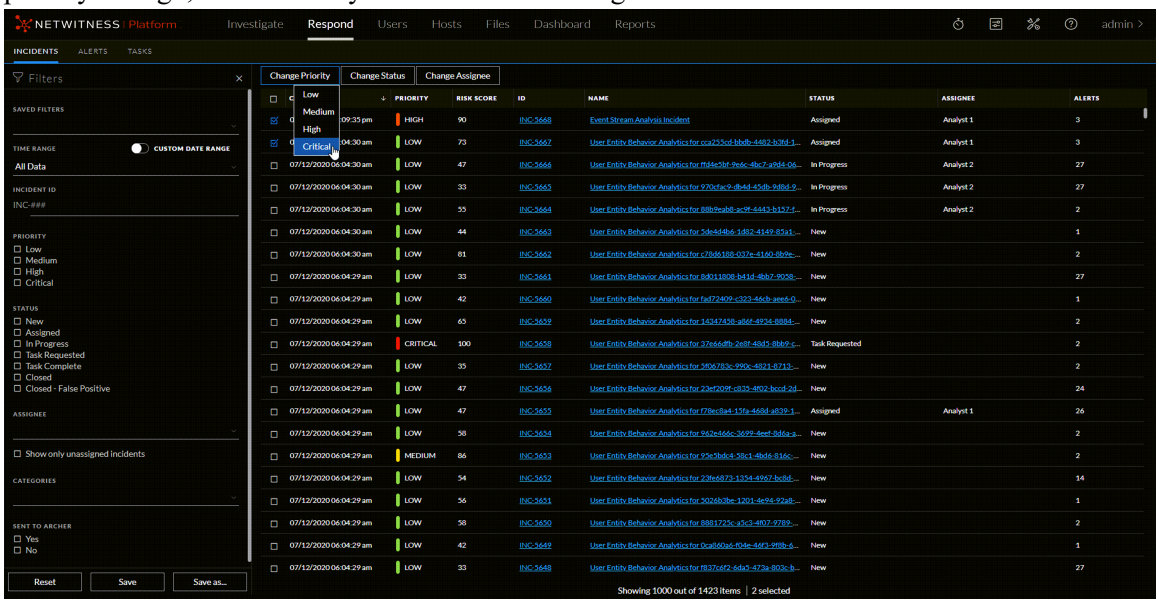
The incident list is sorted by Priority by default. You can update the priority as you study the details of the case. The following priorities are available:

- Critical
- High
- Medium
- Low

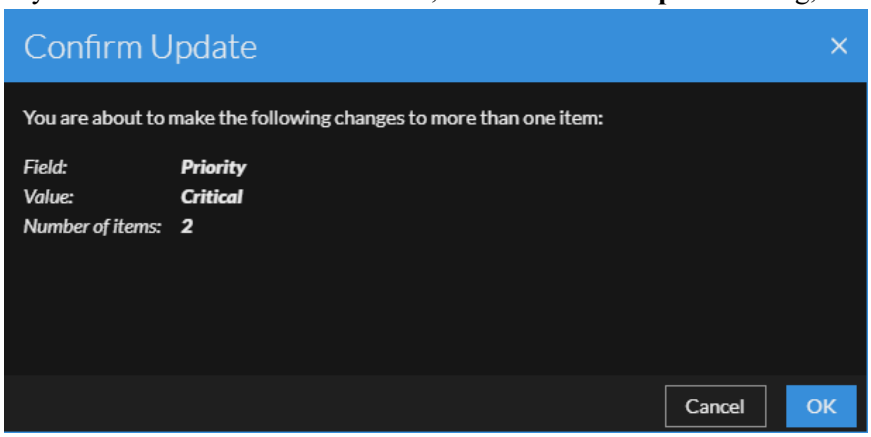
Note: You cannot change the priority of a closed incident.

To update the priority of multiple incidents:

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

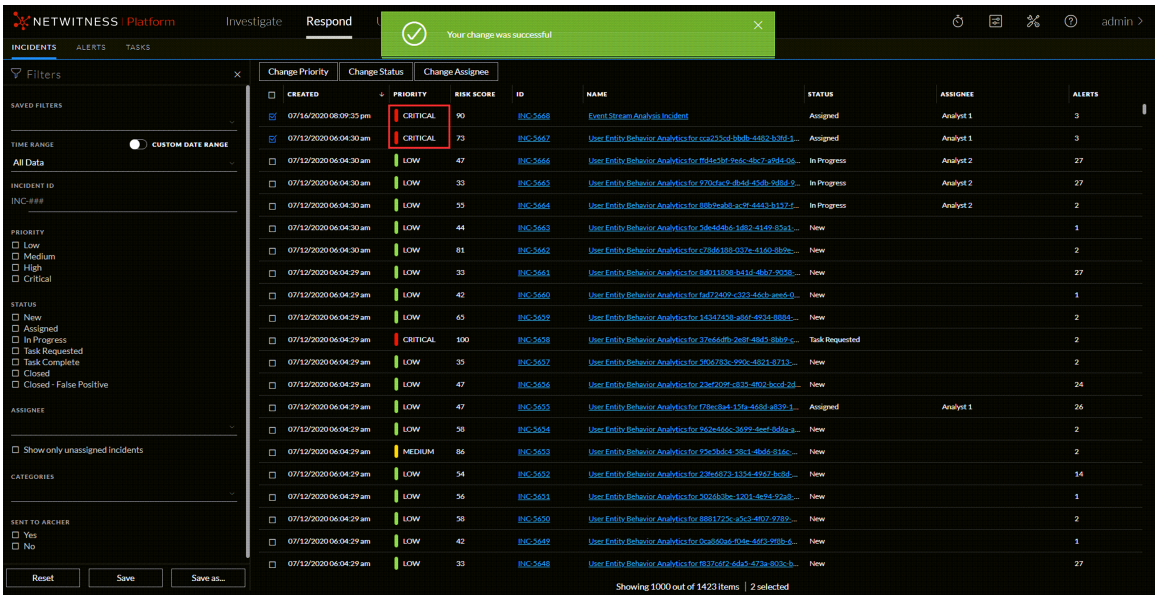


3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.



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

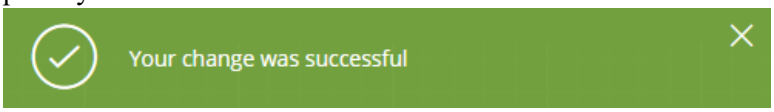
show Critical.



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

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

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



Note: Current priority is grayed out under **Priority** drop-down list. You will not be able to select the grayed out priority.

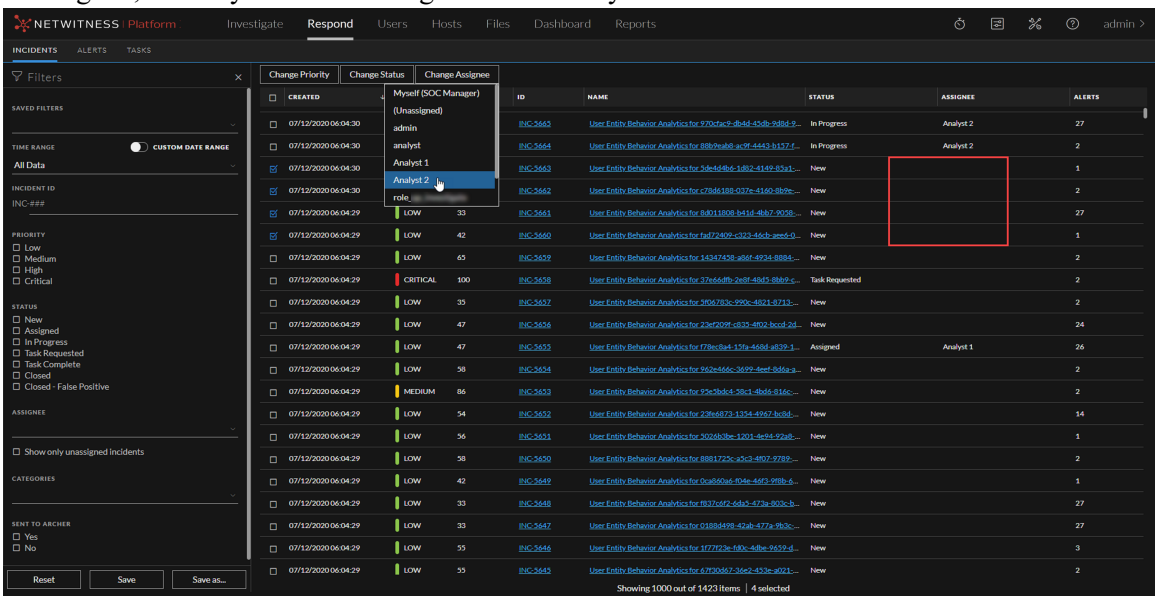
Assign Incidents to Other Analysts

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

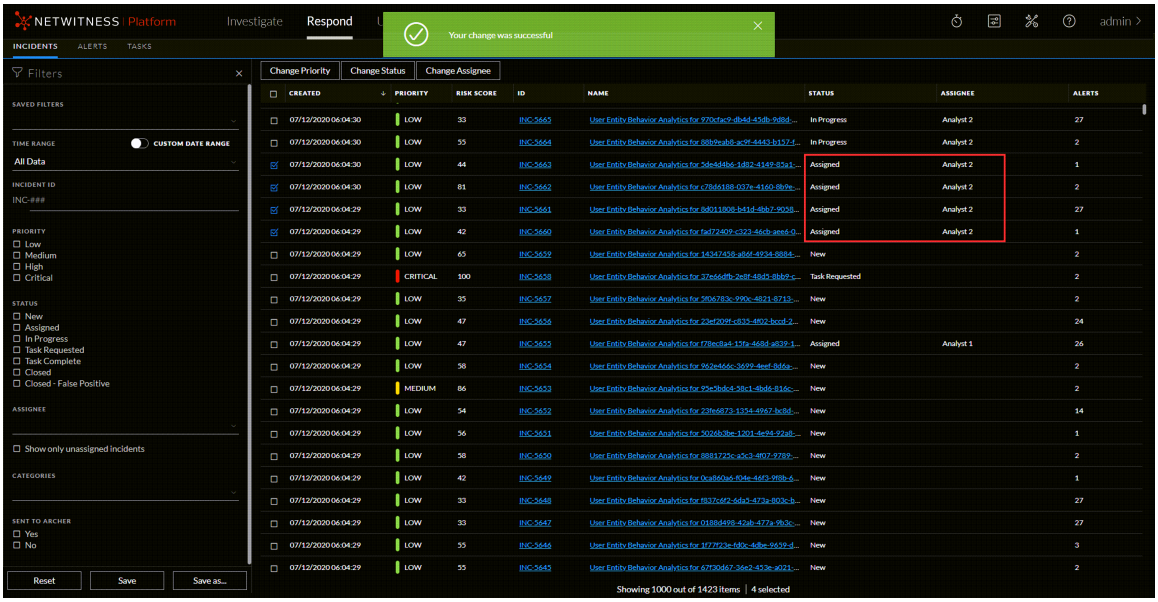
Note: You cannot change the assignee of a closed incident.

To assign multiple incidents to a user:

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



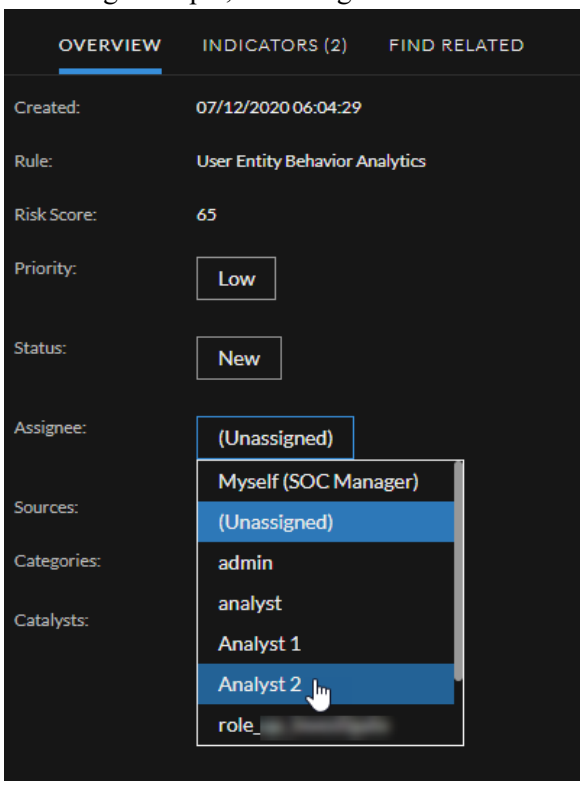
3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.
   You can see a successful change notification. The assignee changes to the selected user.



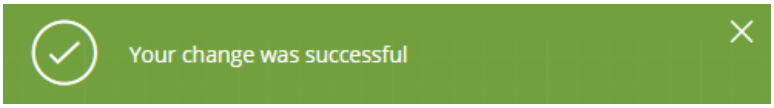
To assign a user to an incident from the Overview panel:

1. To open the Overview panel, do one of the following:
   - From the Incidents List view, click the row of an incident that you would like to assign to a user.
   - From the Incident Details view, click the **Overview** tab in the left panel.
     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.



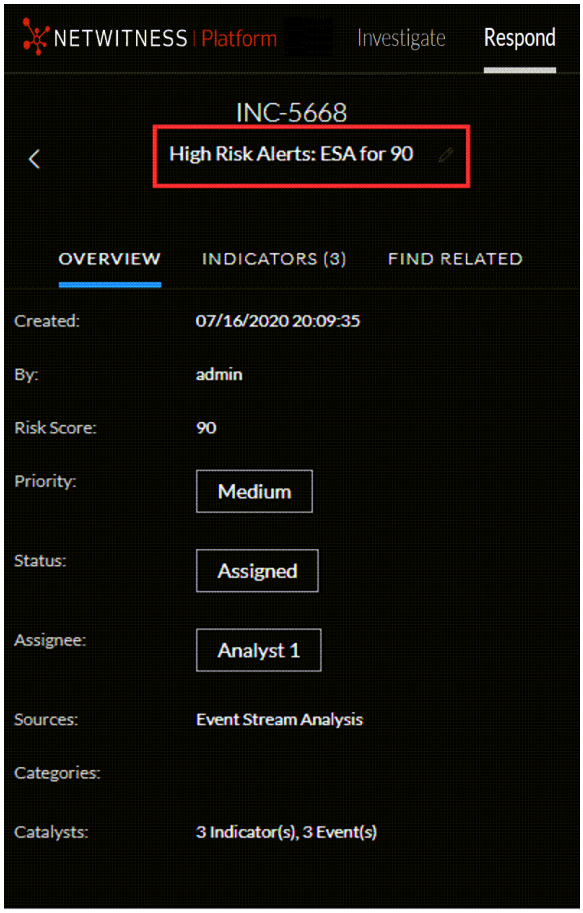
Note: Current assignee name is grayed out under **Assignee** drop-down list. You will not be able to select the grayed out user.

Rename an Incident

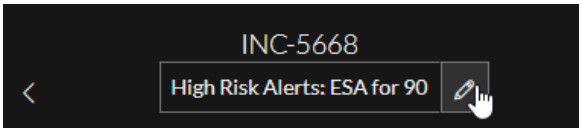
You can rename an incident from the Overview panel in the Incidents List view and the Incident Details view. For example, you may want to rename an incident to provide clarification about the issue, especially if multiple incidents have the same name.

1. Go to **Respond > Incidents**.
2. To open the Overview panel, do one of the following:
   - From the Incidents List view, click the row of an incident that needs a name change.
     The Overview panel opens.

- From the Incident Details view, click the **OVERVIEW** tab in the left panel.
  In the header above the Overview panel, you can see the incident ID and the incident name.

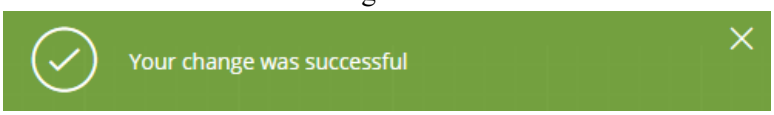


3. Click the incident name in the header to open a text editor.

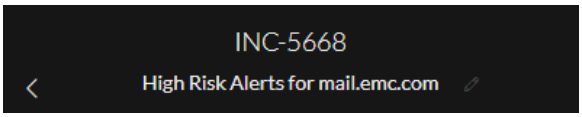


4. Type a new name for the incident in the text editor and click the check mark to confirm the change.

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



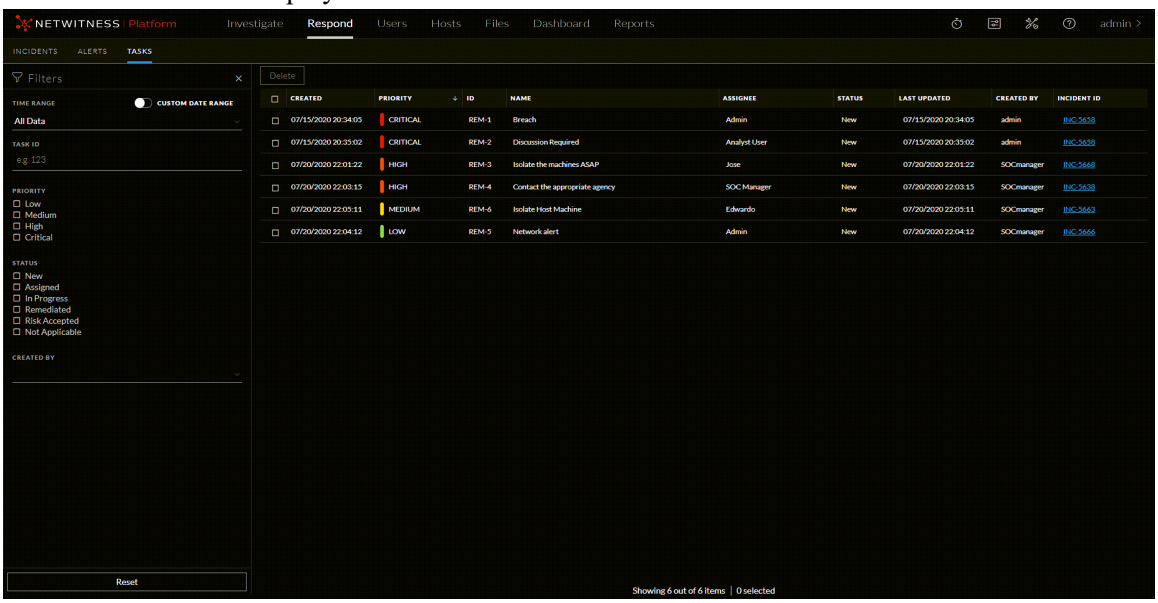
The incident name field shows the new name.



View All Incident Tasks

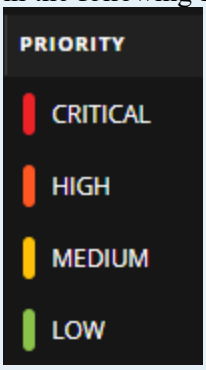
When additional work is required for an incident, you can create tasks for the incident and track the progress on those tasks. This is helpful, for example, when the work being done is outside security operations or you make a request for a computer reimage. In the Tasks List view, you can manage and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

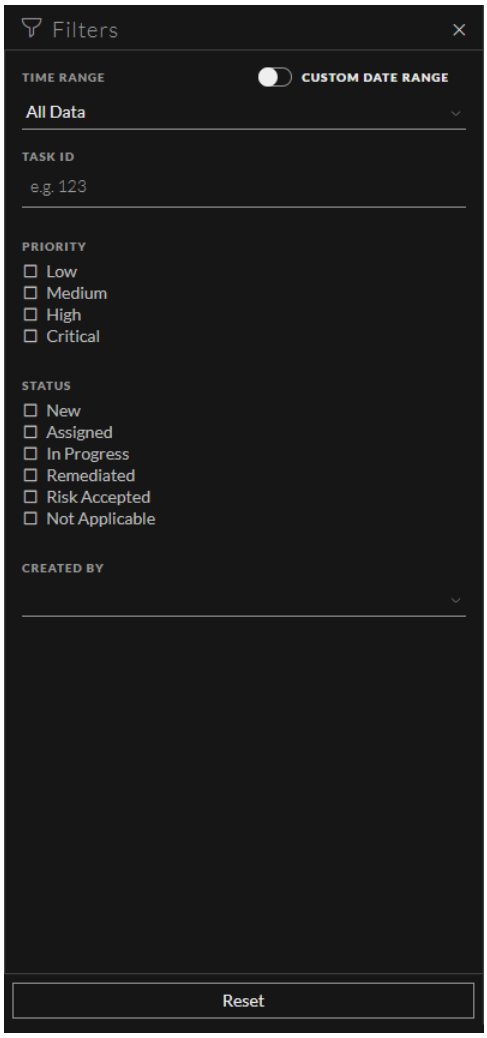
Column	Description
Priority	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates **Critical**, orange represents **High** risk, yellow indicates **Medium** risk, and green represents **Low** risk as shown in the following figure: 
ID	Displays the task ID.
Name	Displays the task name.
Assignee	Displays the name of the user assigned to the task.
Status	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
Last Updated	Displays the date and time when the task was last updated.
Created By	Displays the user who created the task.
Incident ID	Displays the incident ID for which the task was created. Click the ID to display the details of the incident.

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

Filter the Tasks List

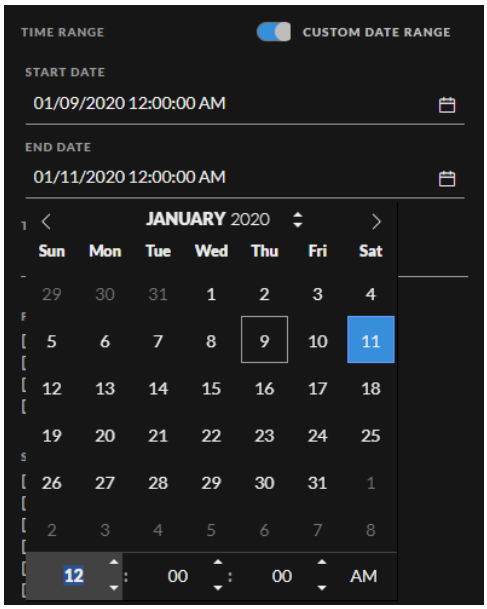
The number of tasks in the Tasks List can be very large, making it difficult to locate particular tasks. The Filter enables you to specify those tasks that you would like to view, such as tasks created within the last 7 days. You can also search for a specific task.

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



2. In the Filters panel, select one or more options to filter the incidents list:
   - **Time Range**: You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the tasks. For example, if you select Last Hour, you 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

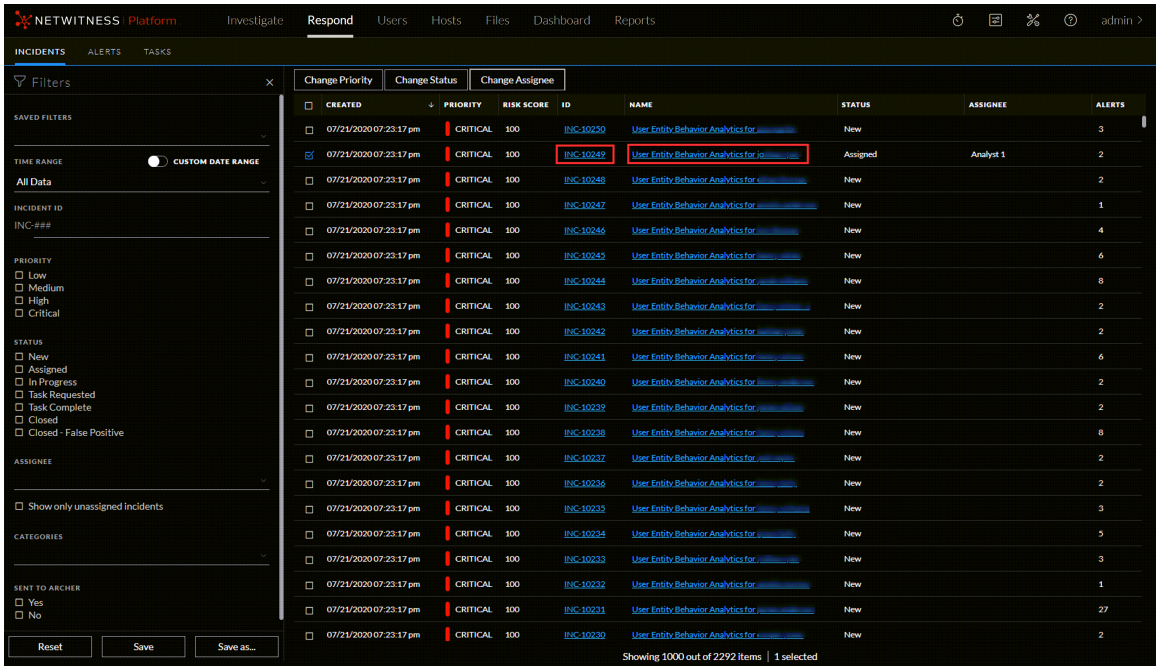
NetWitness remembers your filter selections in the Tasks List view. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of tasks that you expect to see or you want to view all of the tasks in your tasks list, you can reset your filters.

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



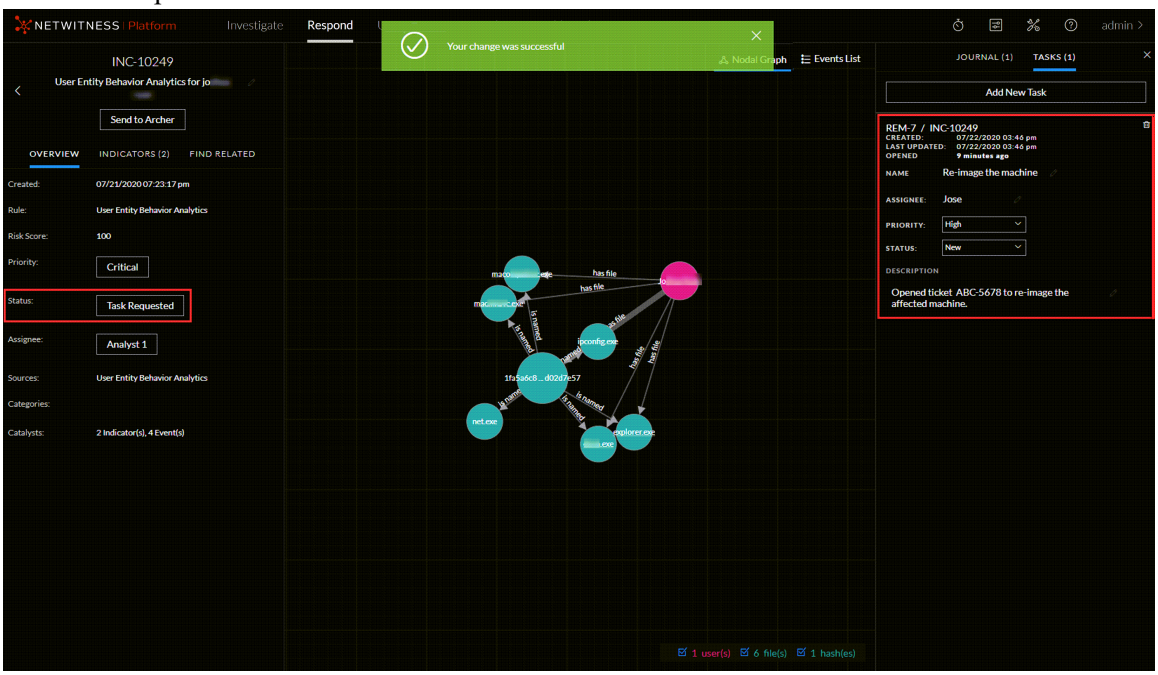
3. In the Journal panel on the right side of the Incident Details view, click the **Tasks** tab.
   If you do not see the Journal panel, click **Journal & Tasks** and then click the **Tasks** tab.

4. In the Tasks panel, click **Add New Task**.

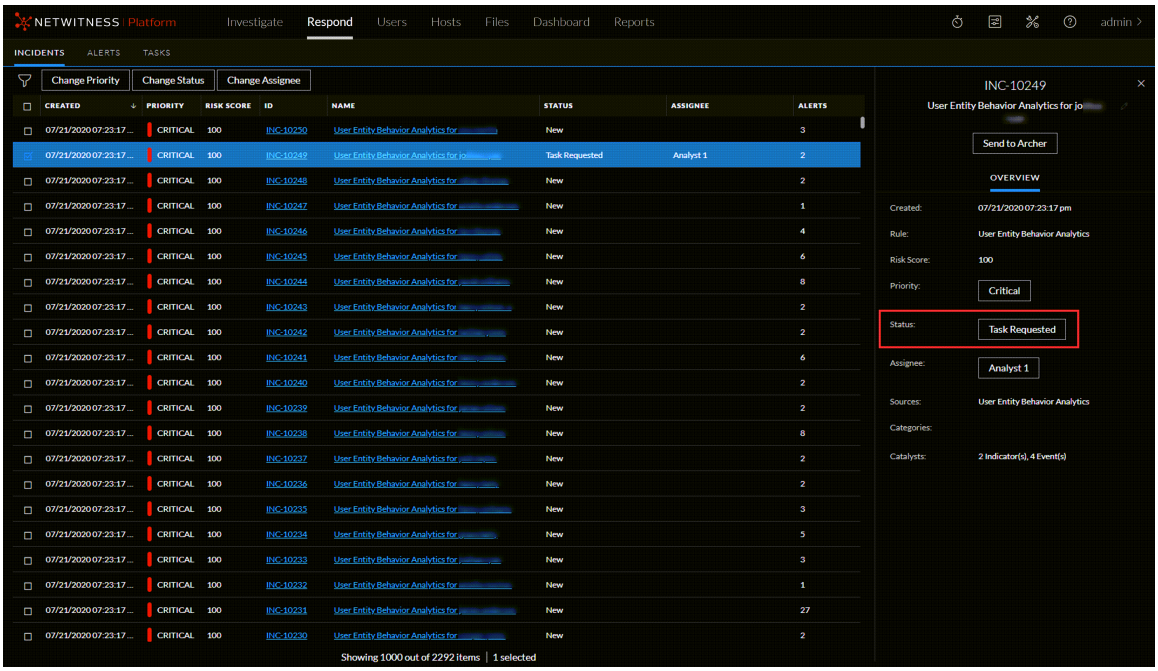
   You can see the new task fields.

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

5. 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.
6. Click **Save**.
   You can see a confirmation that your change was successful. The incident status changes to **Task Requested**. (You may need to refresh the Incident Details view to see the changes.) The task appears in the Tasks panel for this incident.



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



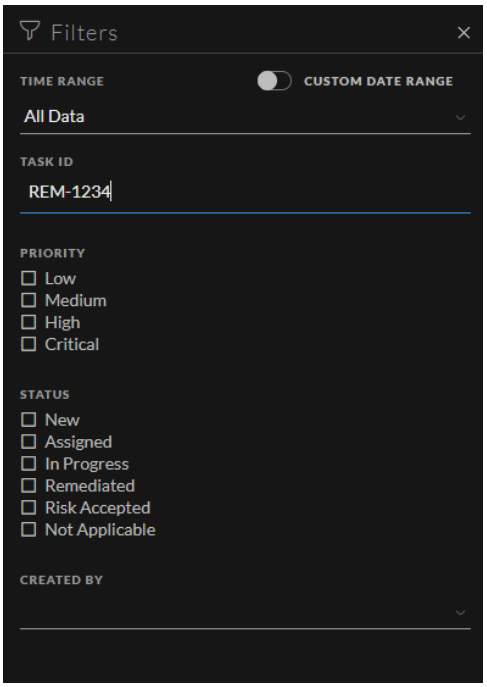
The task also appears in the Tasks list (Respond > Tasks), which shows a list of all incident tasks.

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.

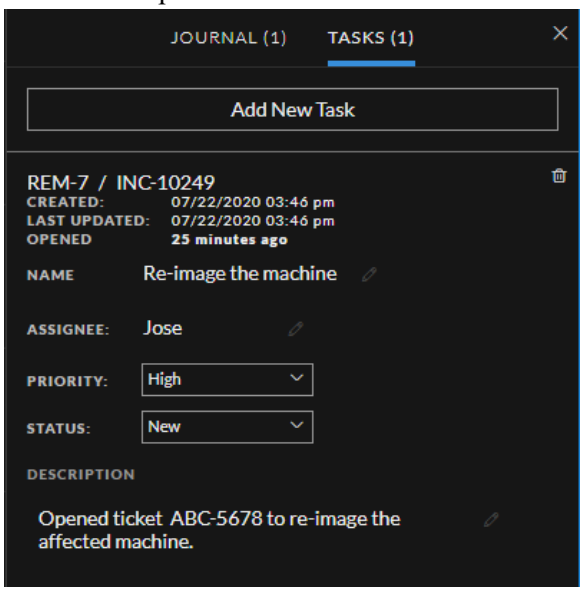
Modify a Task

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:

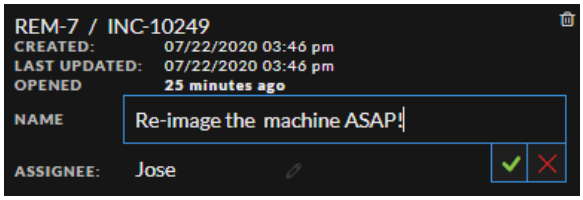
1. Go to **Respond > Incidents**.
   The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **Name** field.
3. In the Journal panel on the right side of the Incident Details view, click the **Tasks** tab.
   If you do not see the Journal panel, click **Journal & Tasks** and then click the **Tasks** tab.
   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.



4. You can modify any of the following fields:

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

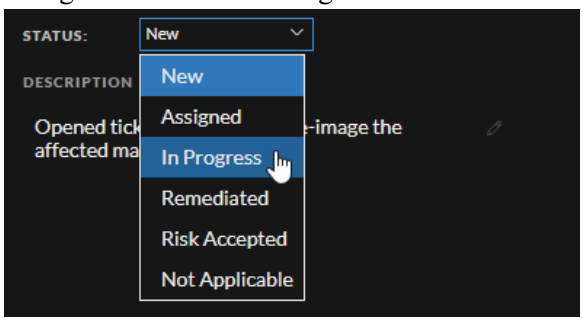


  Click the check mark to confirm the change. For example, you can change "Re-image the machine" to "Re-image the machine ASAP!"

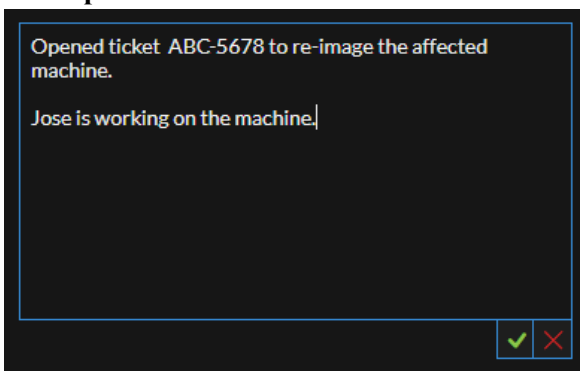
- **Assignee** - Click (Unassigned) or the name of the previous assignee to open a text editor. Type the username of the user to whom the task is to be assigned.
  Click the check mark to confirm the change.

- **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.

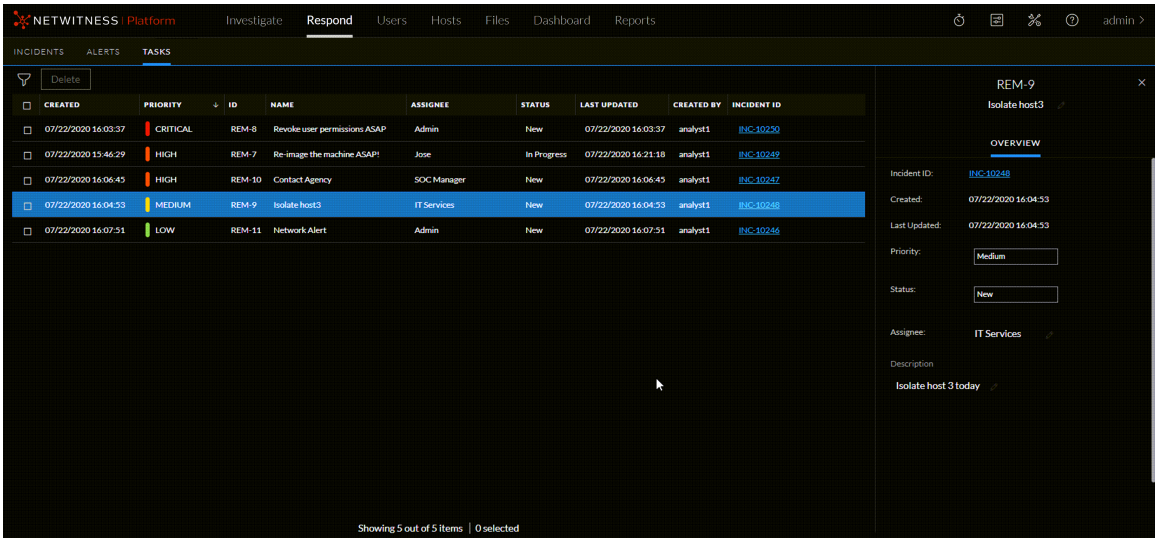


Modify the text and click the check mark to confirm the change.

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

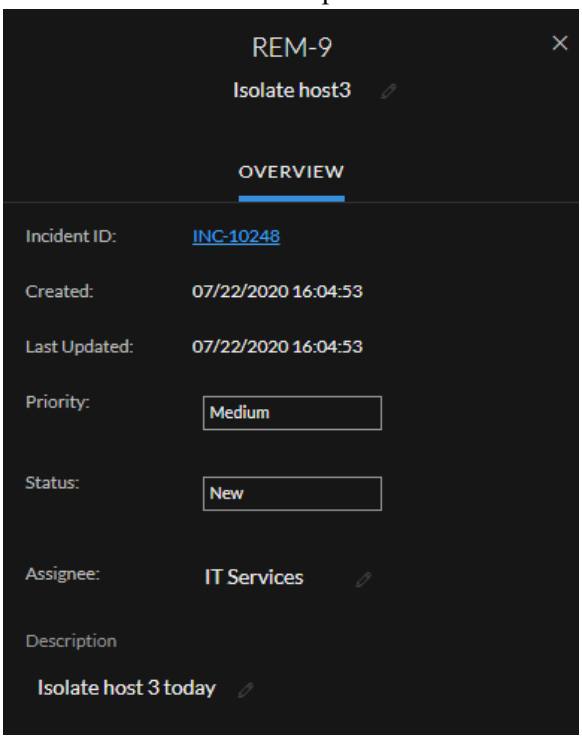
To modify a Task from the Tasks list:

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.



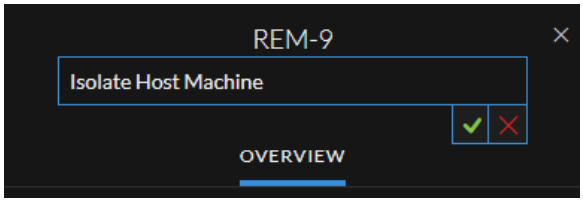
In the Task Overview panel, a pencil icon indicates a text field that you can change. A button

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



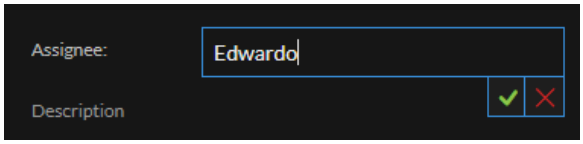
3. You can modify any of the following fields:

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



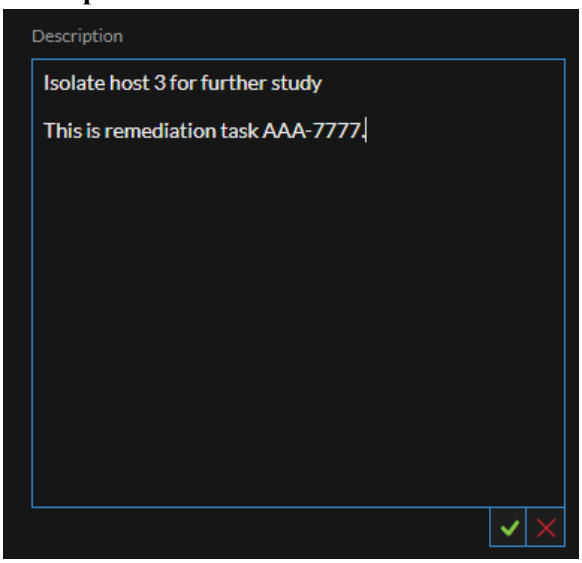
Click the check mark to confirm the change. For example, you can change Isolate Host to Isolate Host Machine.

- **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.

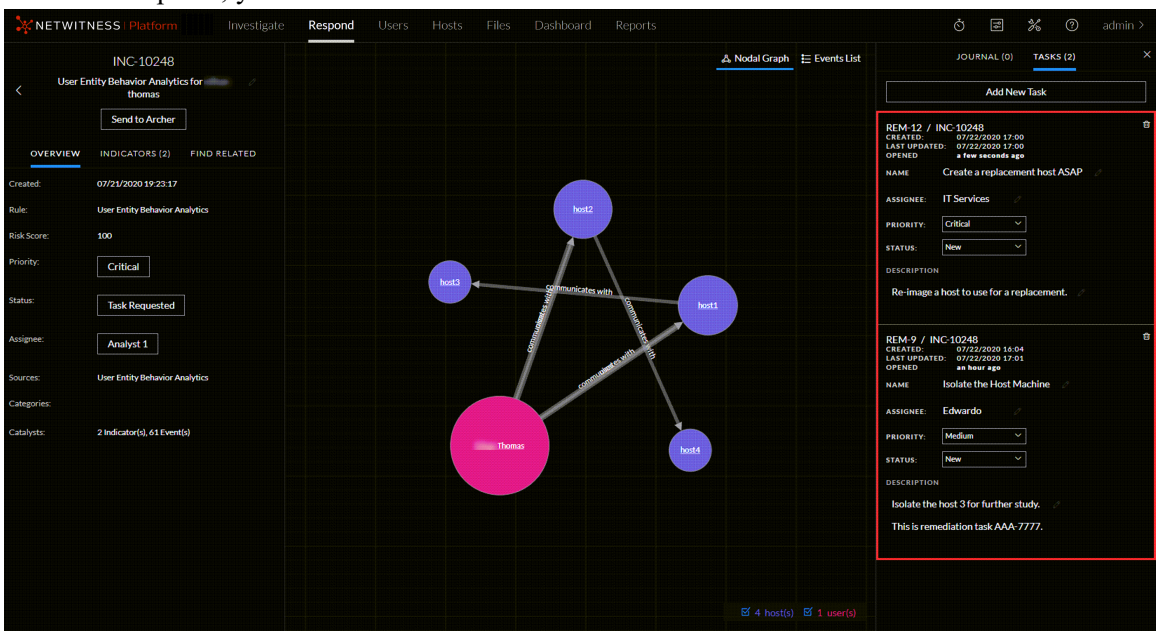
Delete a Task

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.

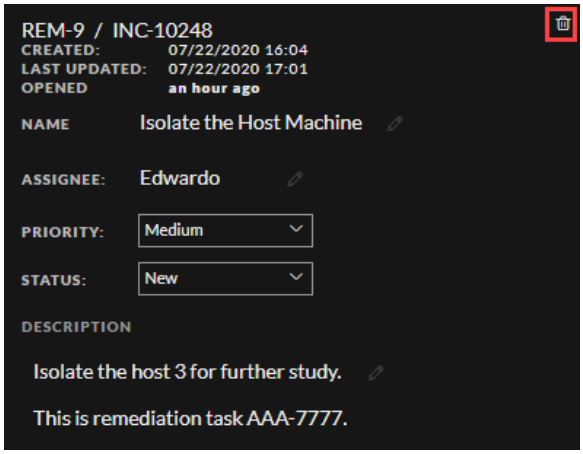
To Delete a Task from within an incident:

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.
3. In the Journal panel on the right side of the Incident Details view, click the **Tasks** tab.
   If you do not see the Journal panel, click **Journal & Tasks** and then click the **Tasks** tab.

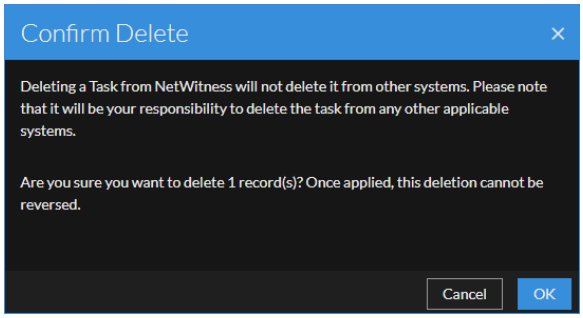
In the Tasks panel, you can see the tasks created for the incident.



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



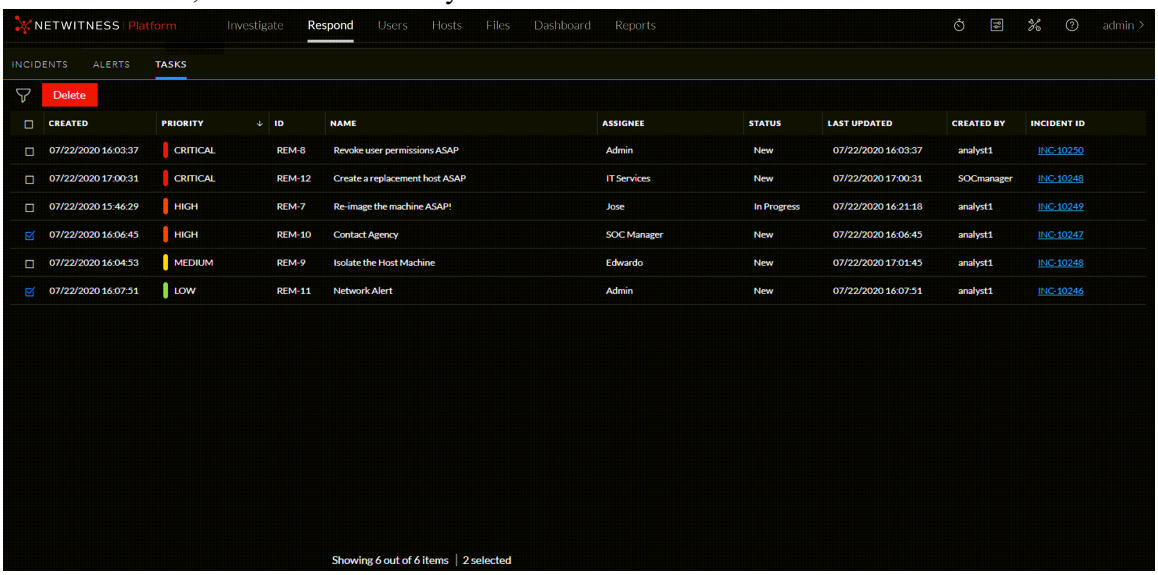
5. Confirm that you want to delete the task and click **OK**.



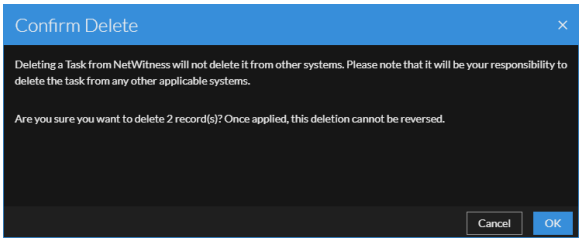
The task is deleted from NetWitness. Deleting tasks from NetWitness does not delete them from other systems.

To Delete Tasks 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, select the tasks that you want to delete and click **Delete**.



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



   The tasks are deleted from NetWitness. Deleting tasks from NetWitness 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.

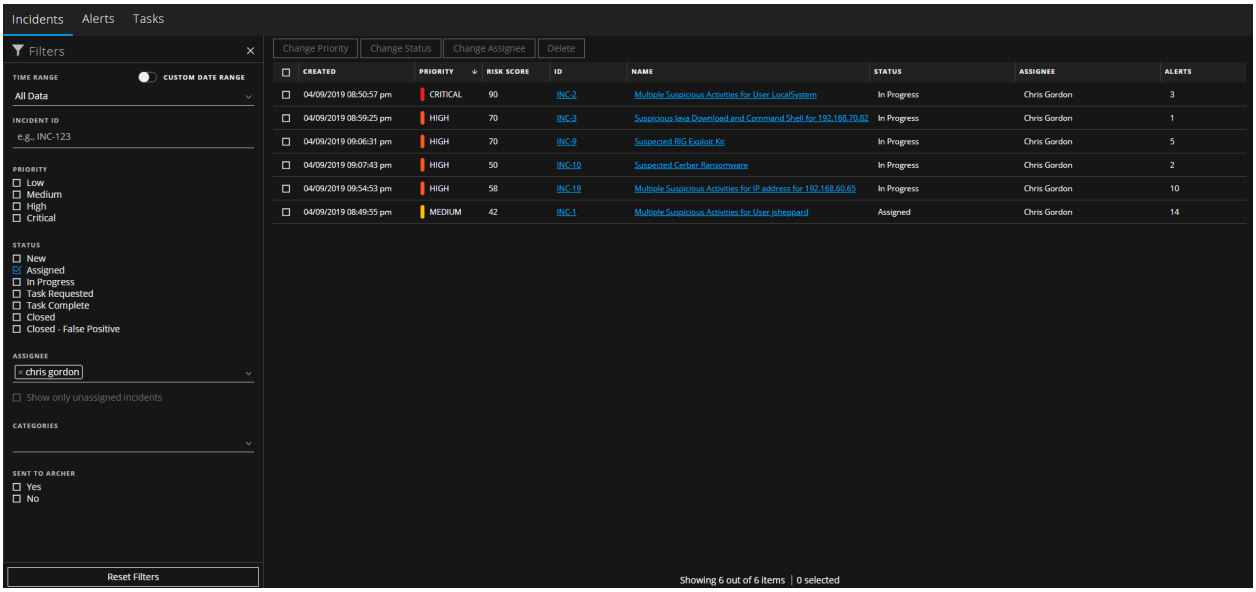
Note: You can also close an incident in the Overview panel. You can close multiple incidents at the same time in the Incident List view. Change Incident Status provides additional details.

Incident Response Use Case Examples

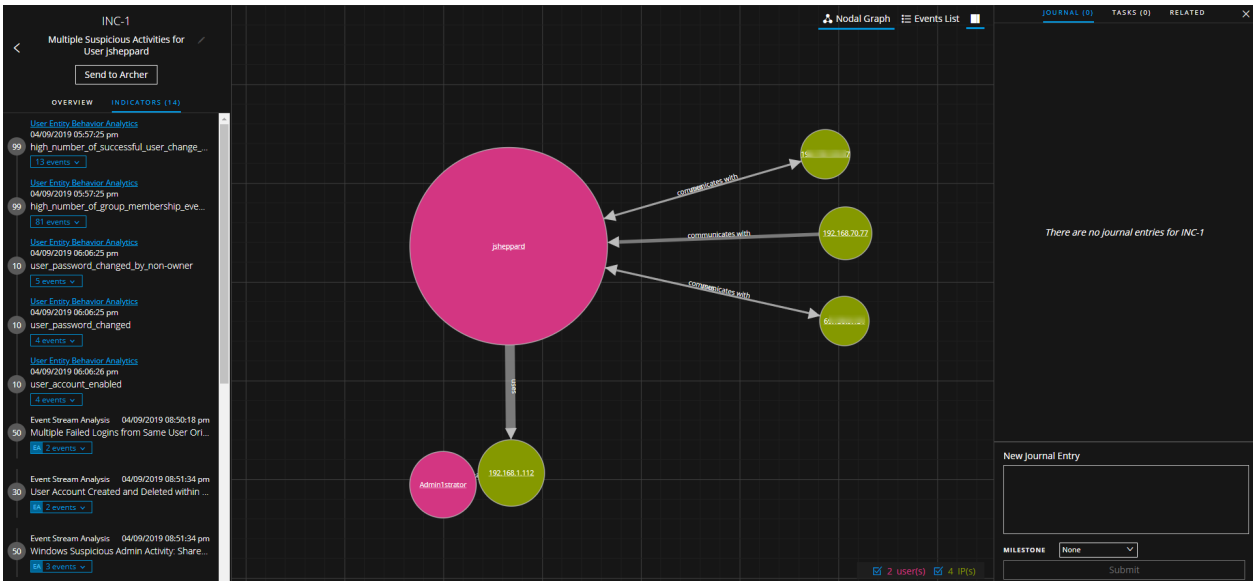
The following use cases provide examples of an analyst using NetWitness to quickly respond to incidents, identify threats, and take action to reduce or eliminate the ability of threat actors to compromise valuable information in the corporate network.

Use Case #1: UEBA Anomalous User Activity

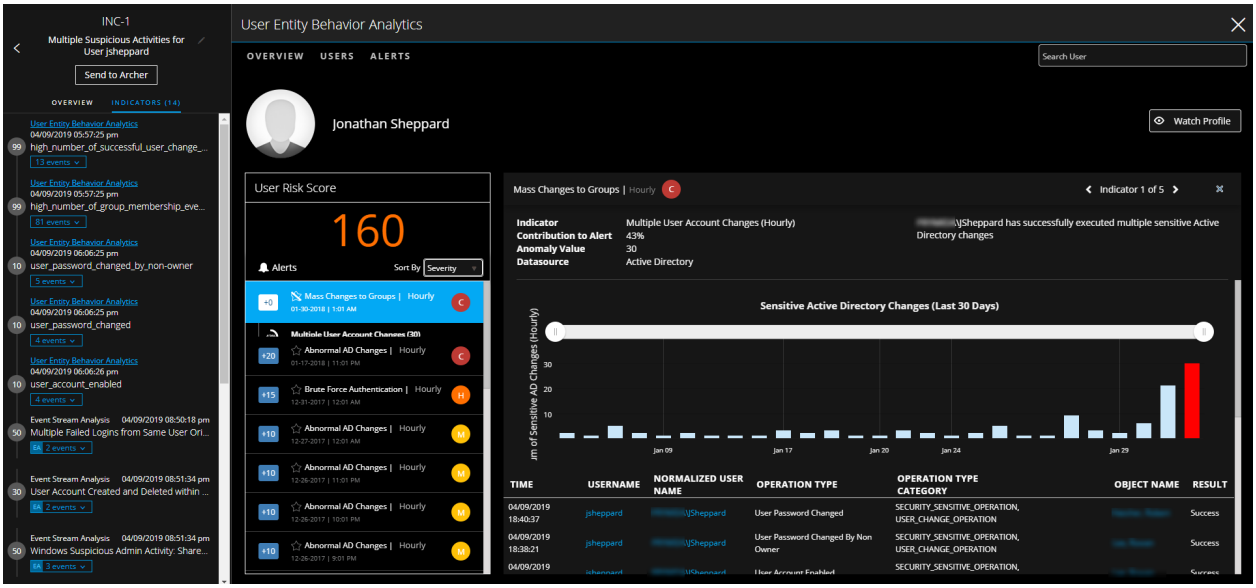
An analyst named Chris logs in, goes to the Incidents List view, and uses the filters on the left-hand side to look at all of the incidents assigned to her. In the list, she notices an incident that she has not yet reviewed (status is Assigned) and opens the incident.



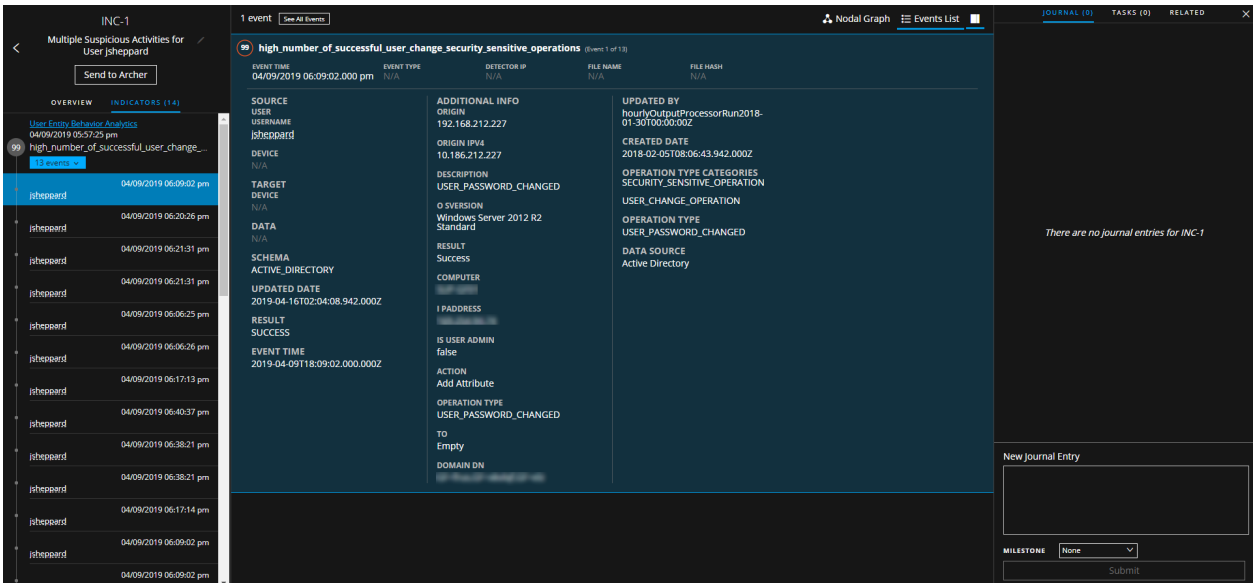
In the Incident Details view, the analyst sees a timeline of contributing events (Indicators panel) on the left, a visualization of the entities involved in the middle, and additional panels on the right where she can keep track of notes and tasks during her review.



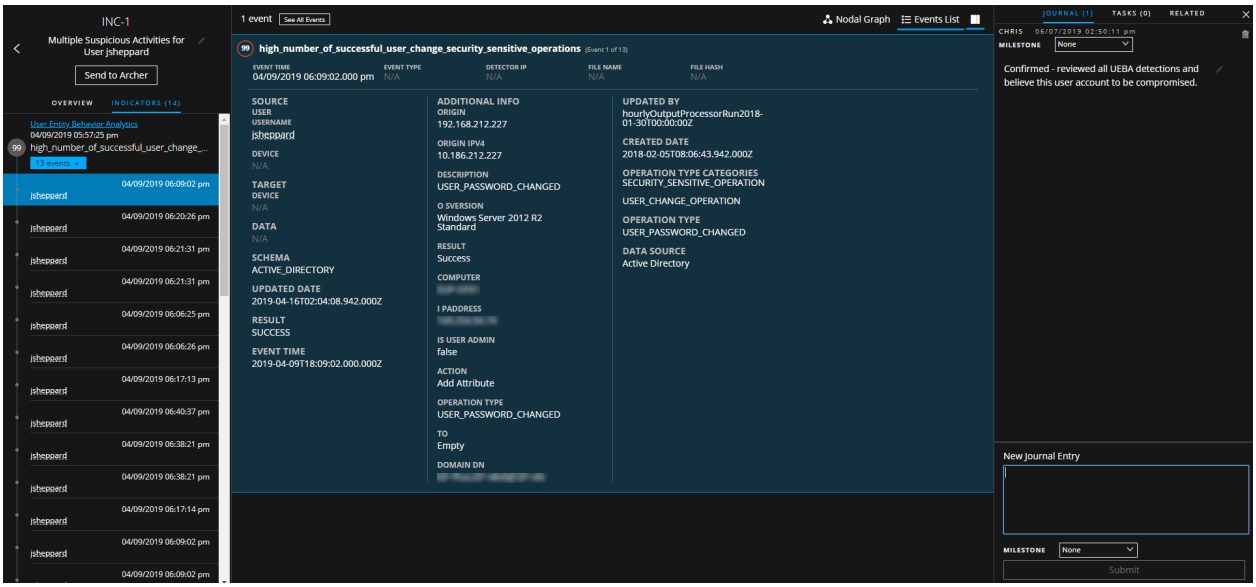
Chris uses the Indicators panel to get finer detail on the events that lead to this incident being created. Clicking the "User Entity Behavior Analytics" link in the Indicators panel exposes the analysis that was done and the anomaly that was detected on the user account "Jonathan Sheppard (jsheppard)." The User Entity Behavior Analytics panel below shows an overall risk score of 160, details the Windows events that contributed to the severity, and shows the actual anomaly in user account changes attributed to this user. She can explore the data in as much depth as required to help validate and understand the alert.



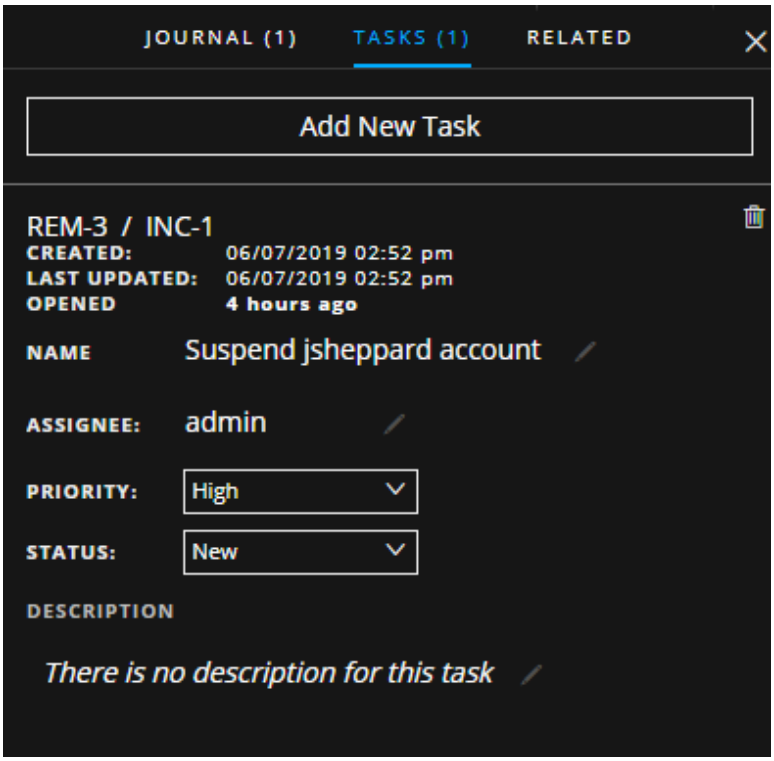
In the Events List, Chris can even inspect the details of the individual log events involved.



During her review and investigation, she can update the incident with her notes, as well as create and assign tasks for herself or other analysts.

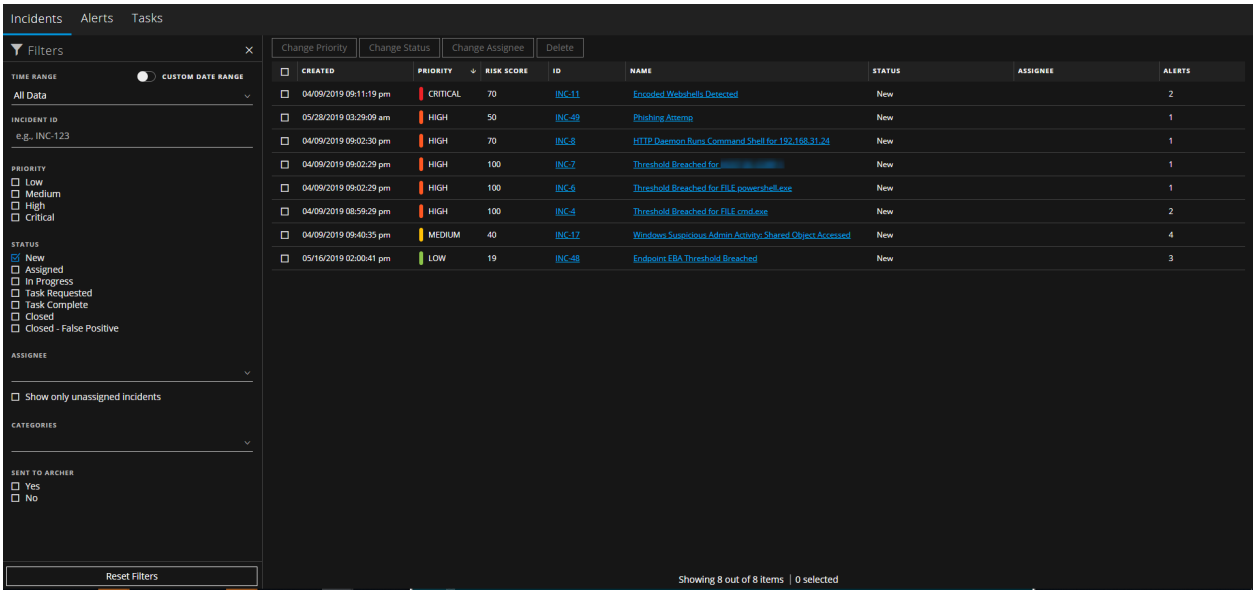


To remediate the incident, Chris opens a task for the administrator (admin) to suspend the jsheppard account.

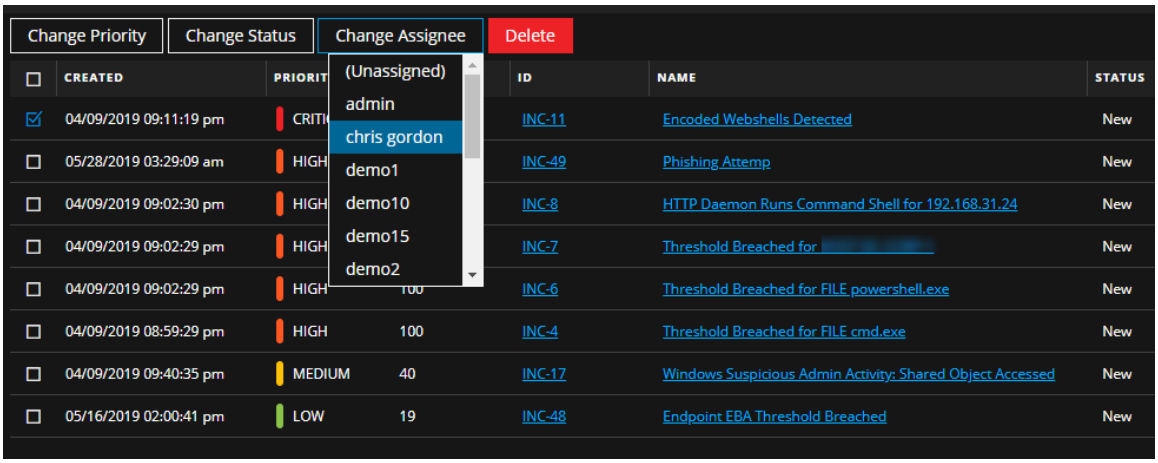


Use Case #2: Encoded Webshells Detected

Analyst Chris logs in, looks at all of the new incidents that have not yet been assigned to anyone, and notices a highly critical incident "Encoded Webshells Detected."

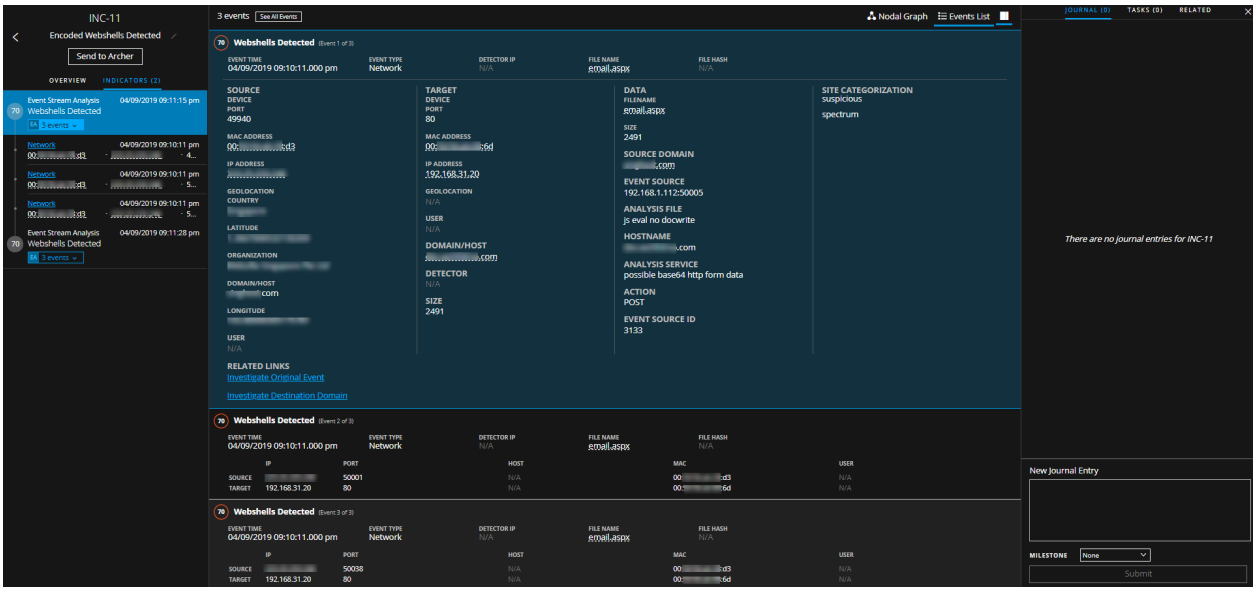


Chris decides to assign this incident to herself and investigate it.

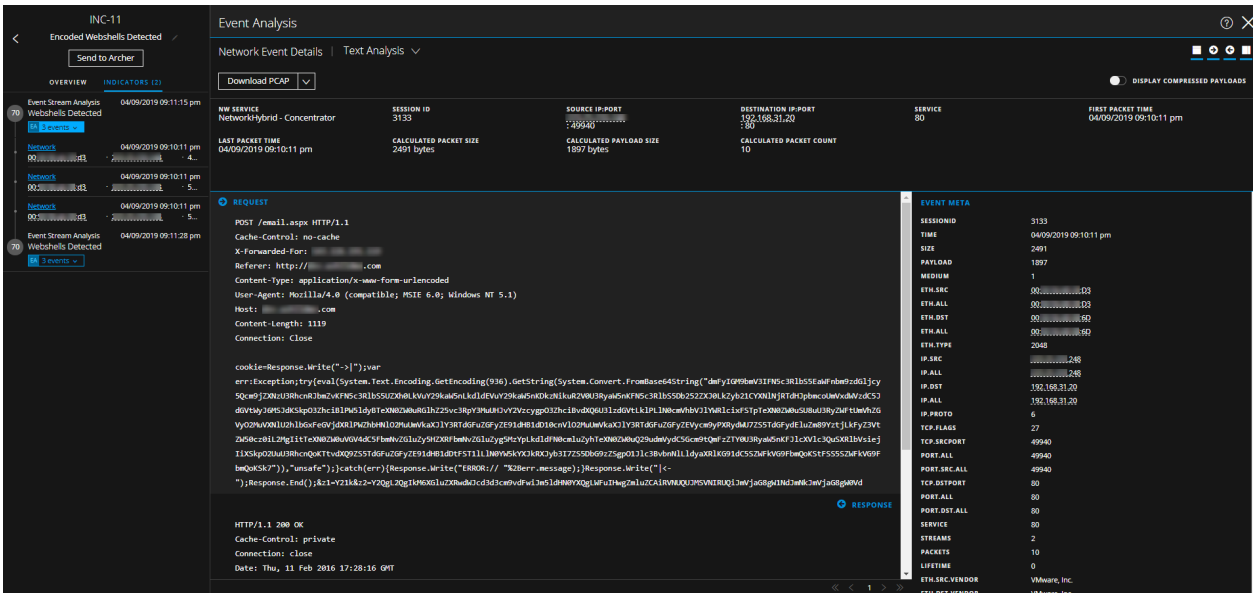


At first glance using the visual summary, Chris can see a couple of specific Event Stream Analysis alerts that kicked off this incident, and the entities associated with the alerts. She sees that a public IP address (xxx.xx.xxx.248) has been detected as interacting with a webshell on the internal web server 192.168.31.20. It looks like the suspicious request was made to the file `email.aspx`. She dives in to investigate.

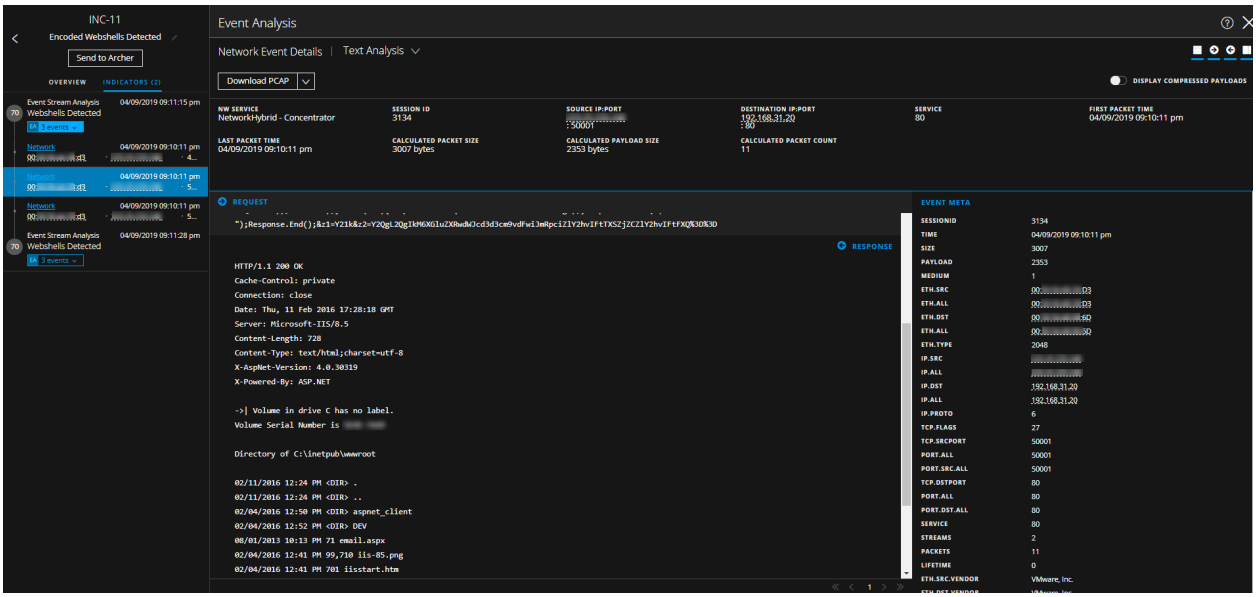
By drilling into the indicator (alert) on the left-hand side, Chris can view the entire list of events associated with the incident and all of the metadata generated by the system, including details about the connections between the external and internal host. She notices that the type of data in this case is "Network," meaning that these events were generated by the full packet capture component of NetWitness.



While the metadata associated with these events does look suspicious to Chris, she wants to investigate even deeper to see what is going on. To do this she can drill into the raw packet reconstruction of the HTTP sessions simply by clicking the "Network" link in the Indicators panel on the left-hand side.

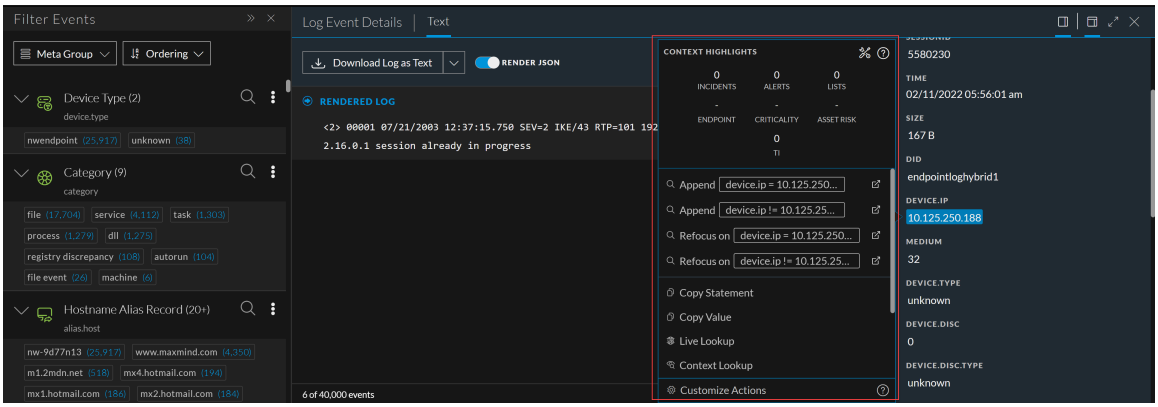


From this deep dive, Chris can examine the raw payload of the suspicious connections and can easily see the strange nature of this request. In the request payload she can see a strange looking request, but most alarmingly, once she scrolls down to the response portion she can see the information that her web server is sending back out to the suspect external IP address.

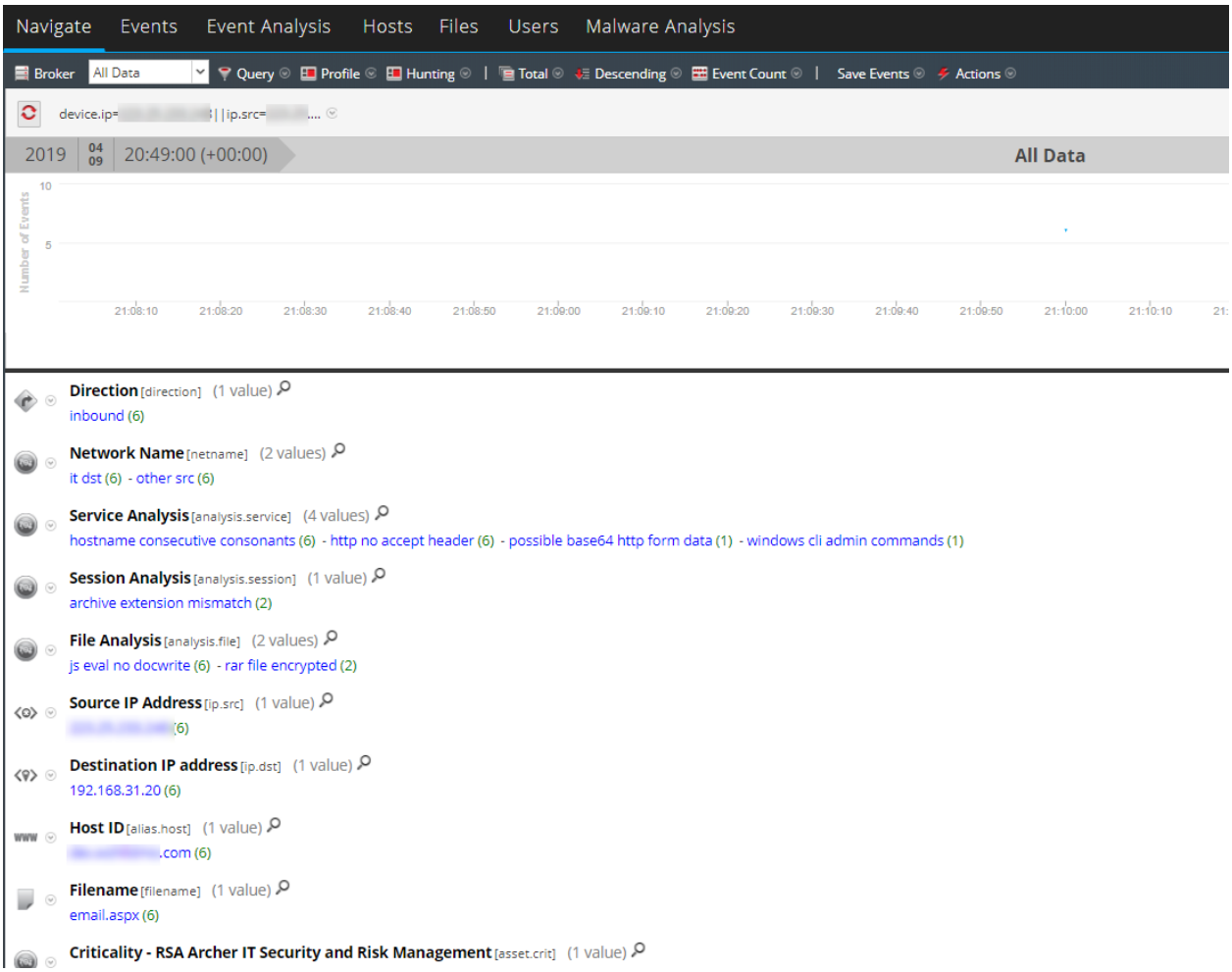


Chris sees what looks to be a directory listing in the packet data, which is not something she would expect from normal web site communications. With this information, she confirms that this is indeed a malicious webshell that has been installed on the internal web server.

From here, Chris can take a number of actions. She can journal her confirmation, assign a task to another user to handle the incident from there, or she can expand her investigation to look for any other activity that has been associated with the malicious external IP address. Chris does this by left or right click the IP address to open a context tooltip and pivoting into Investigate.



This pivot brings Chris into another part of the NetWitness interface where she can perform free-form search and analysis outside of the incident.



In this case she did not uncover anything other than the same network events that were part of the original incident, which is a good step in validating the isolated scope of the incident. If, however, she were to find other interesting events across any log, network, or endpoint data in the system, she could easily add those events into the incident to keep track.

Reviewing Alerts

NetWitness 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, NetWitness Endpoint, NetWitness UEBA (On-premises), NetWitness UEBA (Cloud), NetWitness Insight, 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.

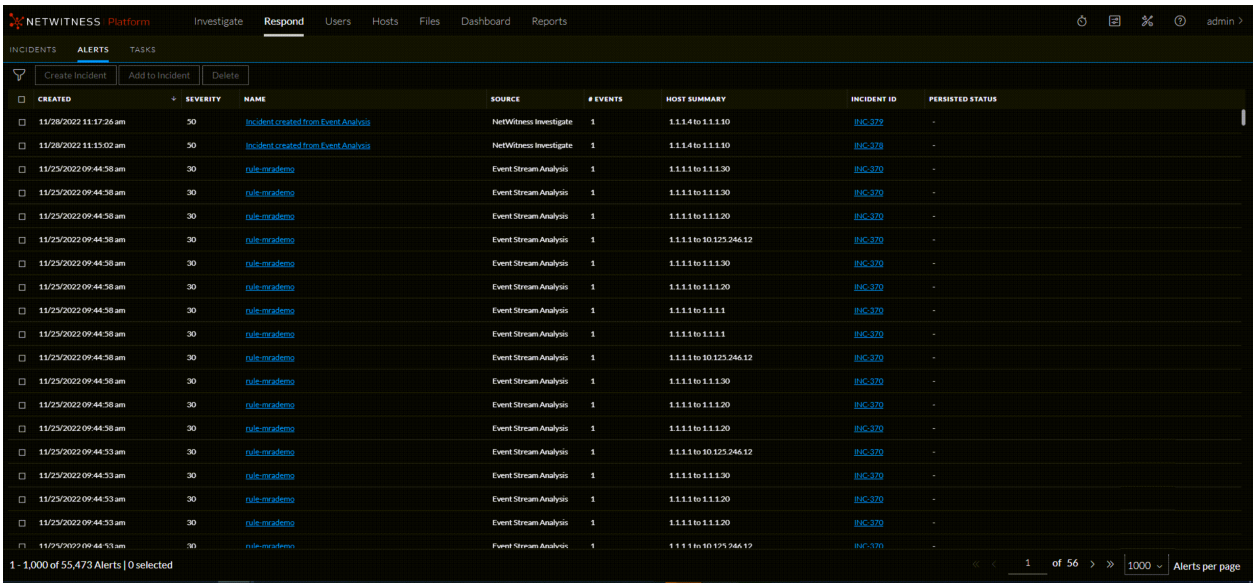
You can perform the following procedures to review and manage alerts:

- View Alerts
- Filter the Alerts List
- Remove My Filters from the Alerts List
- Save the Current Alerts Filter
- Update a Saved Alerts Filter
- Delete a Saved Alerts Filter
- 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 alerts.

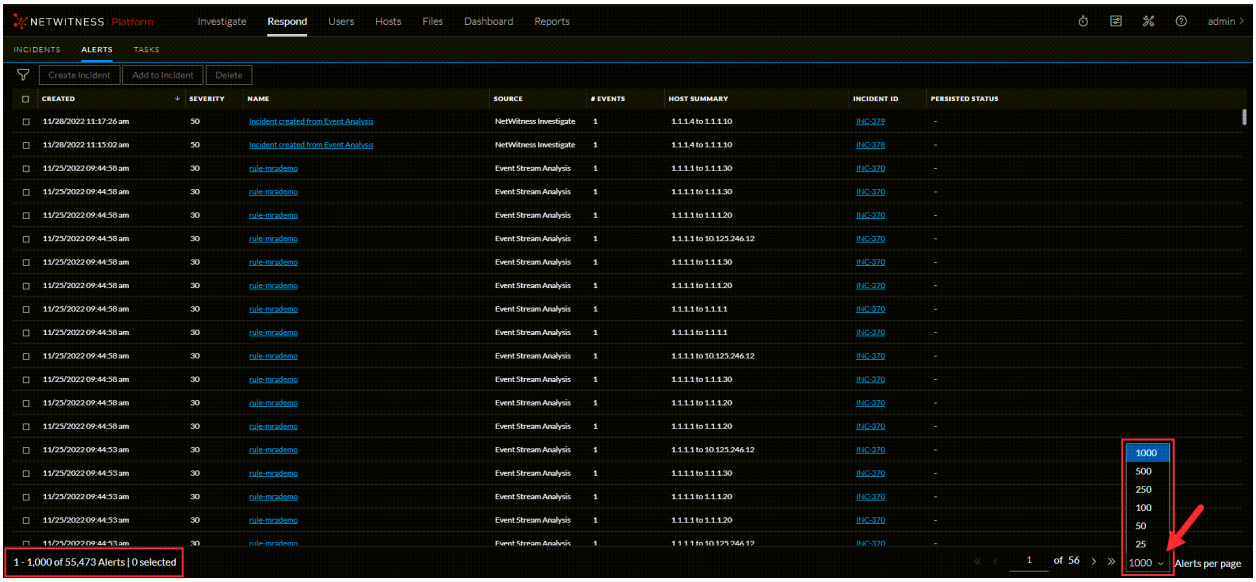


2. Scroll through the alerts list, which shows basic information about each alert as described in the following table.

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, ESA correlation rules, Reporting Engine, Risk Scoring, and many others. **Note:** - From 12.3.1 and later, the alert source filter panel displays only the sources installed in your instance of NetWitness and won't display all possible sources. If a user deletes a host / service on their NetWitness Instance, any source associated with that host / service will be marked as decommissioned. For Ex. ESA Primary is deleted in the hosts page, the ESA source will be marked as decommissioned, the source decommissioned message (**source has been decommissioned**) is displayed in the alert source filter panel.
# Events	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.

Column	Description
Host Summary	Displays details of the host like the host name from where the alert was triggered. The details may include information about the source and destination hosts in an Alert. Some alerts may describe events across more than one host .
Incident ID	Shows the Incident ID of the alert. If there is no incident ID, the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.
MITRE ATT&CK Tactics	Shows the particular Tactic associated with each alert.

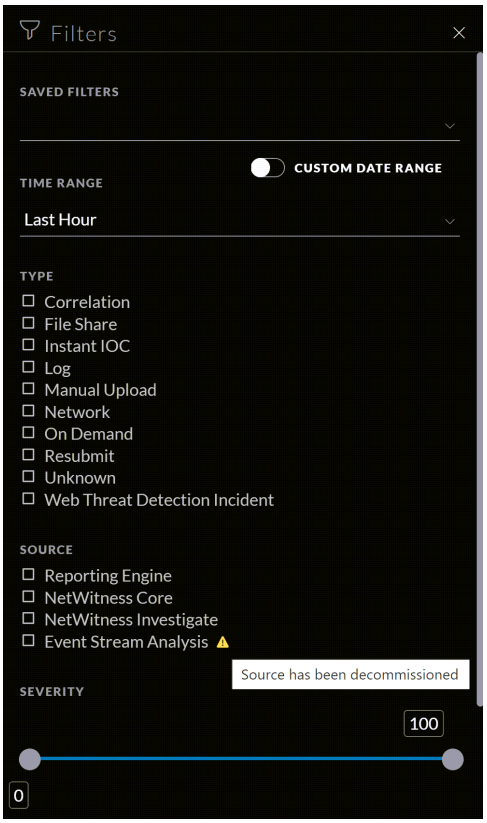
At the bottom of the list, you can see the number of alerts on the current page and the total number of alerts. For example: **1 - 500 of 2400 Alerts | 0 selected**. The maximum number of alerts that you can view at one time is 1,000. You can also change the maximum number of alerts per page by selecting from the drop-down at the bottom right corner.



Filter the Alerts List

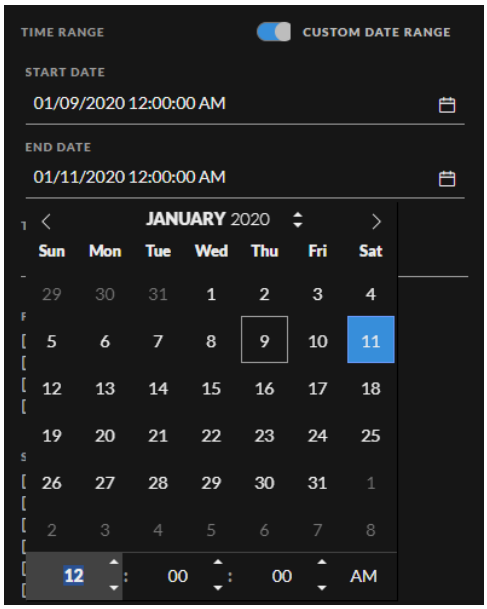
The number of alerts in the Alerts List can be very large, making it difficult to locate particular alerts. The Filter enables you to view the alerts you want to see, for example, alerts from a particular source, alerts of a particular severity, alerts that are not part of an incident, and so on.

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



2. In the Filters panel, select one or more options to filter the alerts list:
   - **Time Range**: You can select a specific time period from the Time Range drop-down list. The time range is based on the date that the alerts were received. For example, if you select Last Hour, you 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**: Displays only the alert sources which are installed. 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. Netwitness Core is available from 12.3 and later version. 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, for example, Direct Login to an Administrative Account.
- **MITRE ATT&CK Tactics**: Select the tactic associated with the alert.
- **MITRE ATT&CK Techniques**: Select the technique associated with the alert.

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 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**.

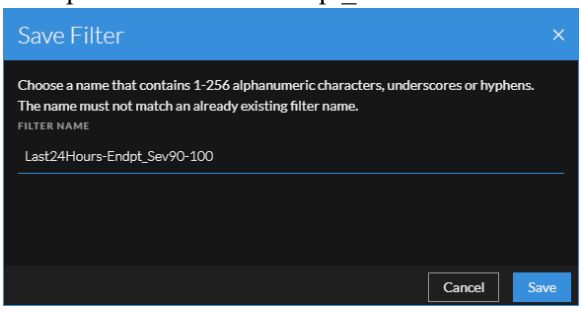
Save the Current Alerts Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

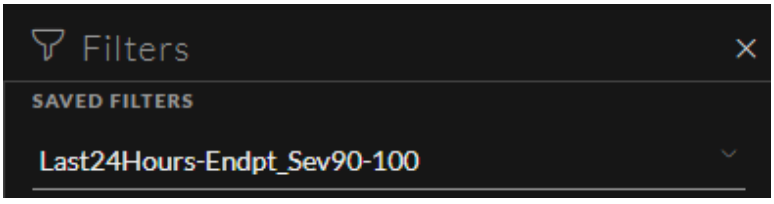
Saved filters provide a way for analysts to save and quickly apply specific filter conditions to the list of alerts. You can also use these filters to customize the Springboard landing page. For example, you may want to create a filter to show only alerts from a specific source and severity level over the last 24 hours. (This option is available in NetWitness Platform 11.5 and later.)

Saved filters are global. You can save a filter for other analysts to use and you can use any saved filter.

1. In the Filters panel, select one or more options to filter the incidents list. For example, in the Time Range field select Last 24 Hours, in the Source field select Endpoint, and for Severity, select the 90 to 100 range.
2. Click **Save As** and in the **Save Filter** dialog, enter a unique name for the filter and save it, for example Last24Hours-Endpt_Sev90-100.



The filter is added to the **Saved Filters** list.



Update a Saved Alerts Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

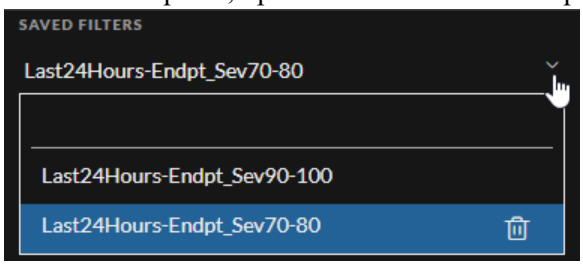
1. In the Filters panel **Saved Filters** drop-down list, select a saved filter.
2. Update your filter selections and click **Save**.

Delete a Saved Alerts Filter

Note: This option is available in NetWitness Platform Version 11.5 and later.

When a saved filter is no longer required, you can remove it from the saved filters list. Filters used in the Springboard cannot be deleted.

1. In the Filters panel, open the **Saved Filters** drop-down list.

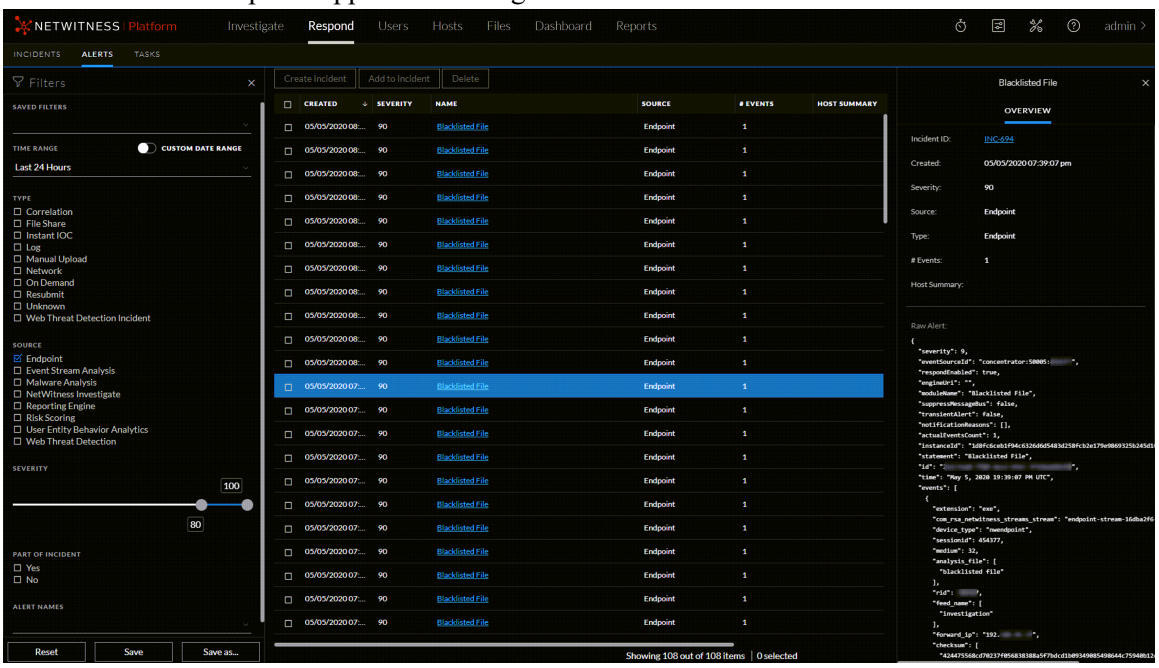


2. Next to the filter name, click  to delete it.

View Alert Summary Information

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

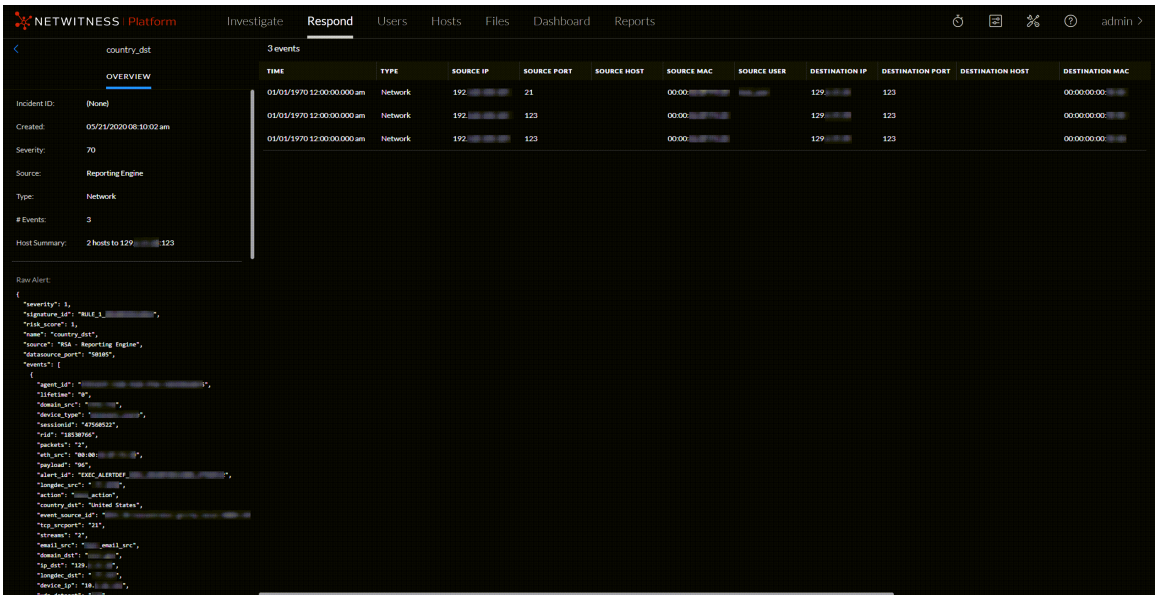
1. In the Alerts list, click the alert that you want to view.
   The Alert Overview panel appears to the right of the Alerts list.



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 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:

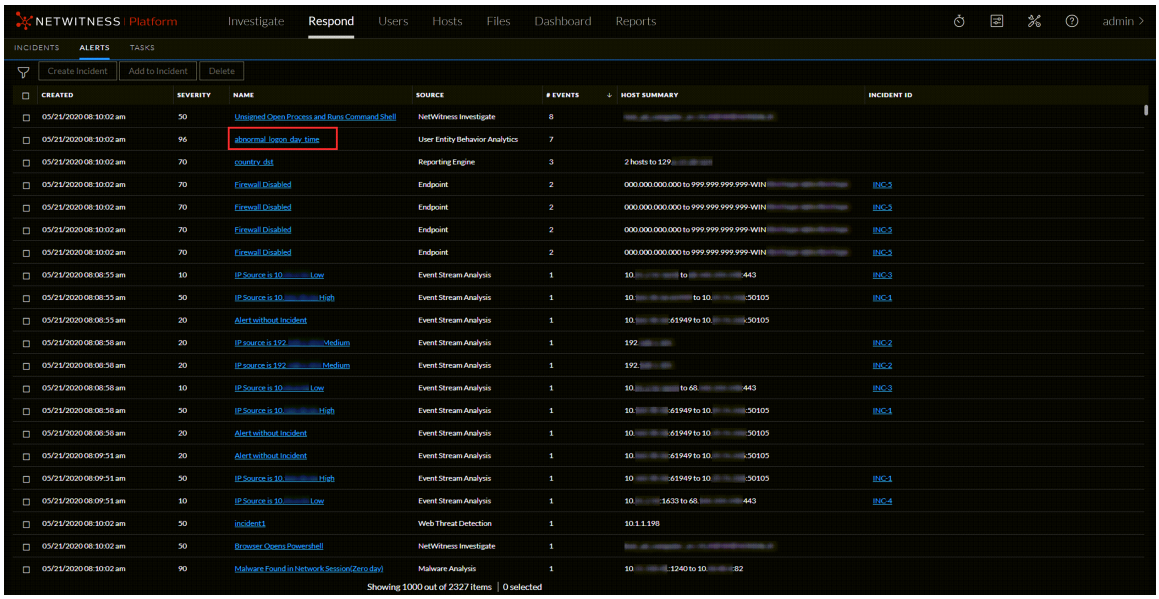
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

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.

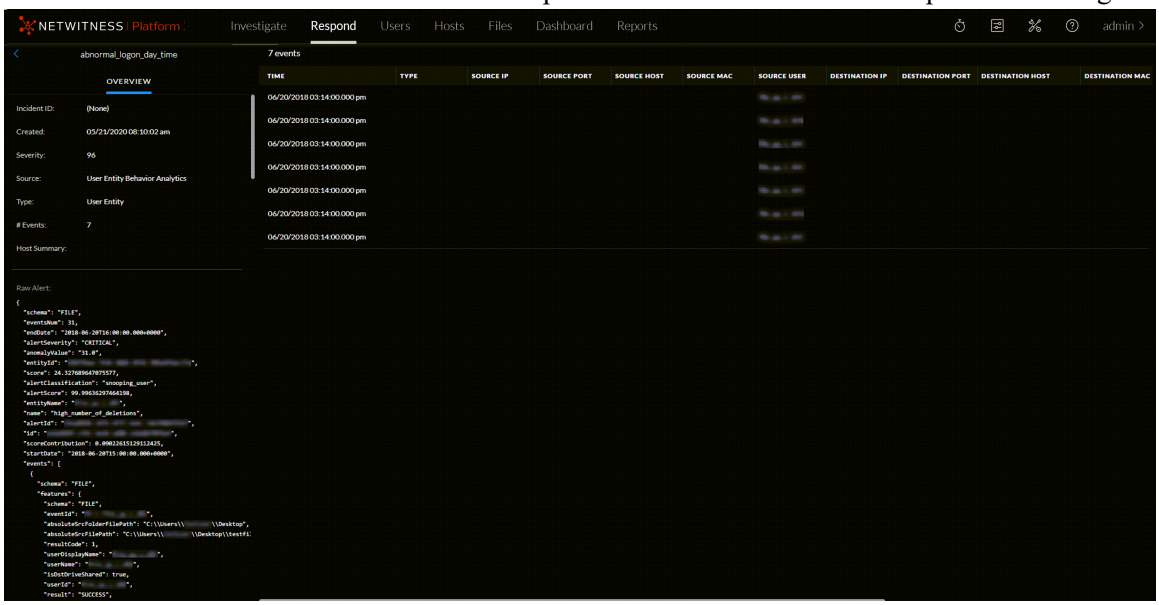
You can drill further into an event to get detailed data about the event.

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.



The Alerts Details view shows the Overview panel on the left and the Events panel on the right.



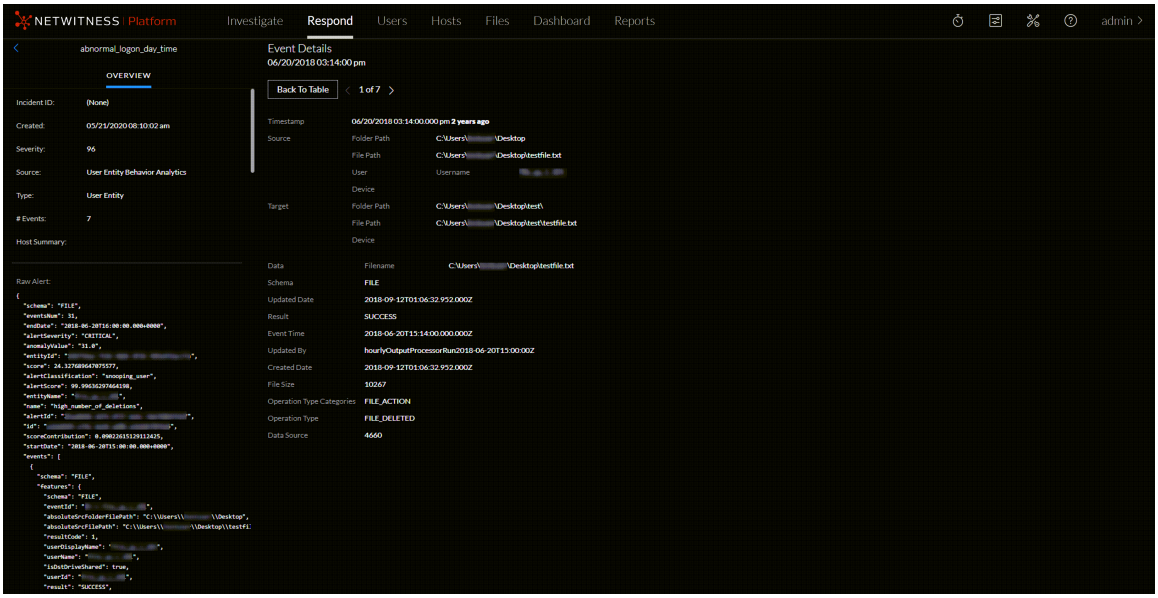
The Events panel shows a list of events with information about each event. The following table shows some of the columns that can appear in the Events List (Events Table).

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.
Destination IP	Shows the destination IP address if there was a transaction between two machines

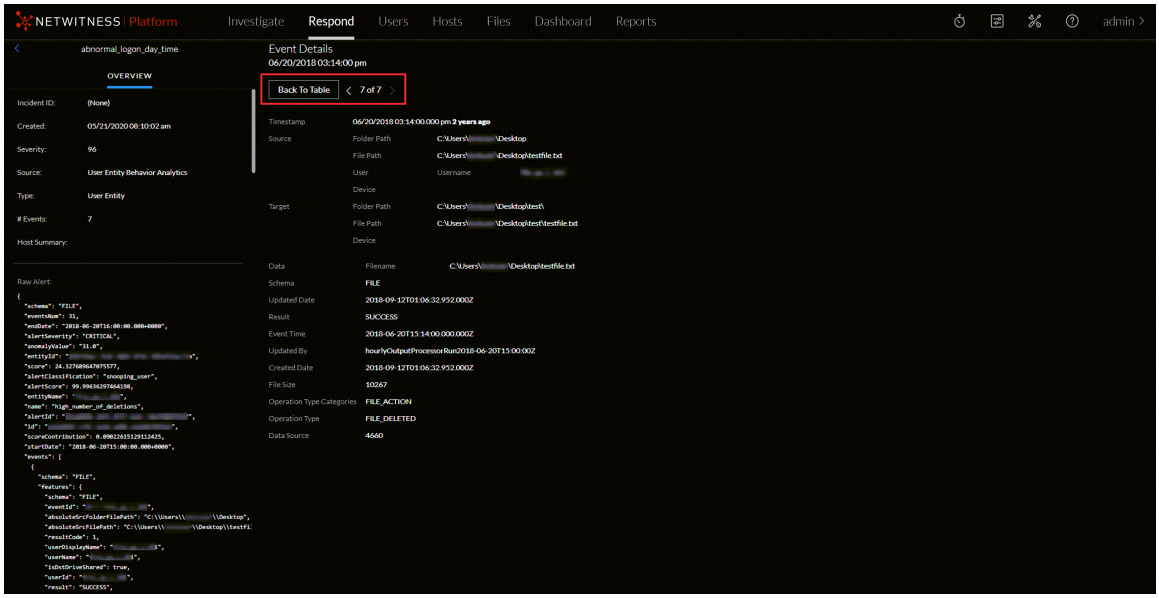
Column	Description
Detector IP	Shows the IP address of the machine where an anomaly was detected.
Source User	Shows the user of the source machine.
Destination User	Shows the user of the destination machine.
File Name	Shows the file name if a file is involved with the event.
File Hash	Shows a hash of 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.

2. Click an event in the Events list to view the Event details.
This example shows the event details for the first event in the list.



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



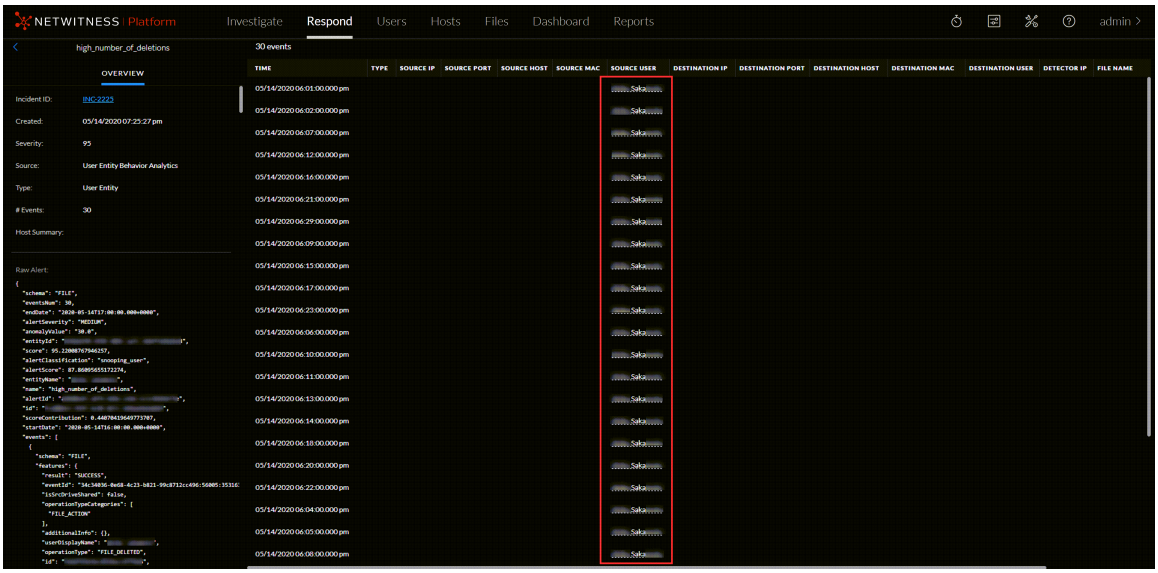
See Alert Details Panel for detailed information about the event data listed in the Alert Details panel.

Investigate Events

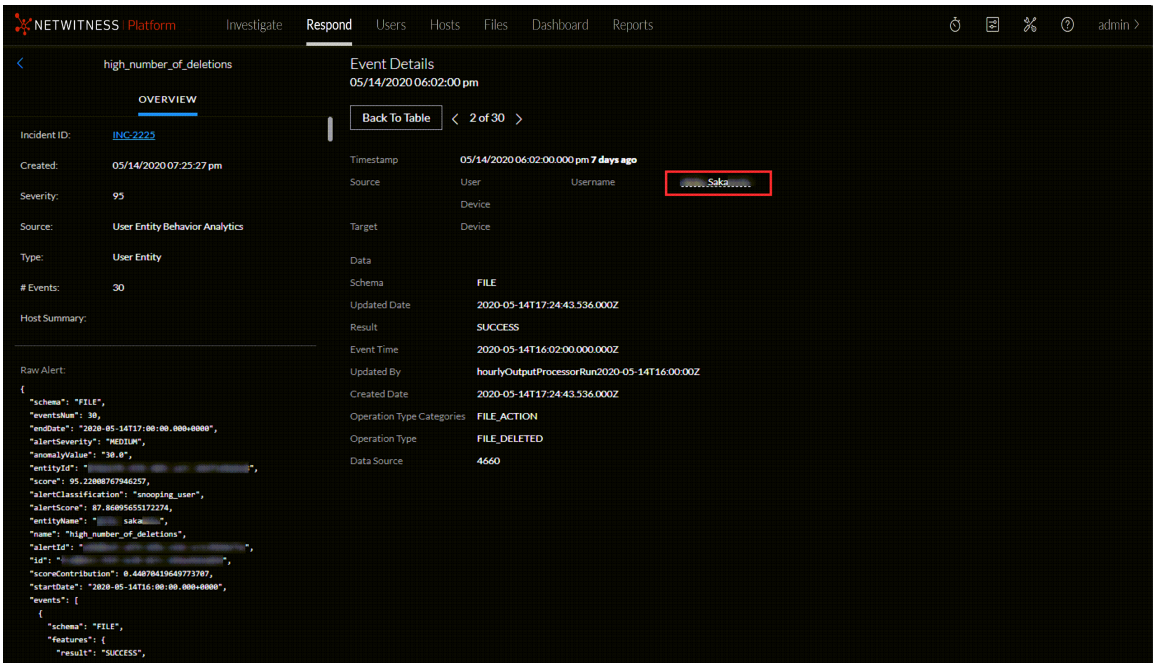
To further investigate the events, you can find links that take you to additional contextual information. From there, you have options available depending on your selection.

View Contextual Information

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



The following figure shows an underlined entity in the Event Details.

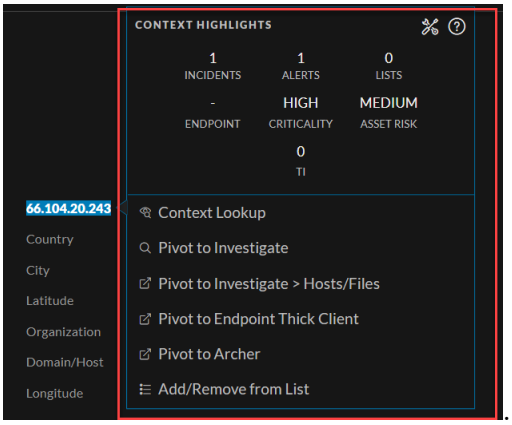


The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and NetWitness Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, NetWitness recommends that when mapping meta keys in the **(missing or bad snippet) > 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, left or right click 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 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. It can show related data for Incidents, Alerts, Lists, Endpoint, Criticality, Asset Risk, Reputation, and Threat Intelligence (TI). Depending on your data, you may be able to click these numbered items for more information. The above example shows 1 related incidents, 1 related alerts, and one list associated with the selected IP address. There is no information for Endpoint, , Criticality, or Asset Risk. TI information comes from the STIX data source configured in Context Hub. For more information, see the *Context Hub Configuration Guide*.

   The other section lists the available actions. In the above example, the Add/Remove From List, Pivot to Investigate, Pivot to Investigate > Hosts/Files, Pivot to Endpoint Thick Client, and and Pivot to Archer 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 Archer configuration is enabled and configured properly.

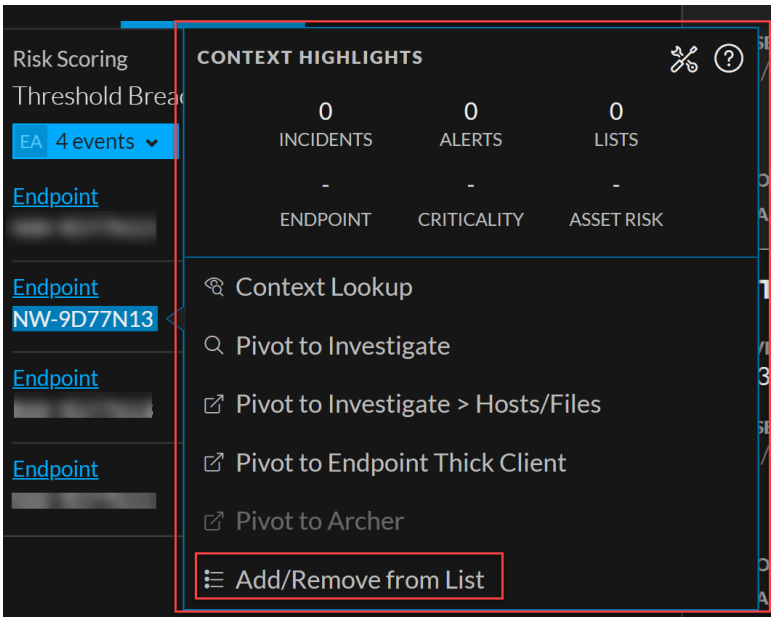
   For more information, see Pivot to the Investigate > Events View, Pivot to the Hosts or Files View, Pivot to Archer, Pivot to Endpoint Thick Client, and Add an Entity to a Whitelist.

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.

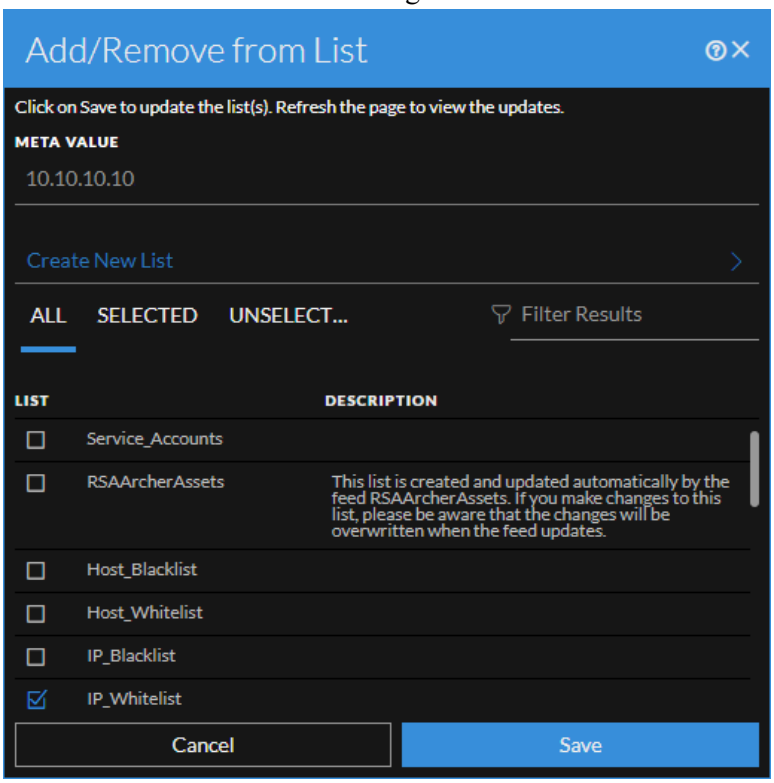
Add an Entity to a Whitelist

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, left or right click the underlined entity that you would like to add to a Context Hub list.
   A context tooltip appears showing the available actions.



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



3. Select one or more lists and click **Save**.
   The entity appears on the selected lists.
   Add/Remove from List Dialog provides additional information.

Create a Whitelist

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

Pivot to the Investigate > Events View

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** > **Events**.
   The Navigate view opens, which enables you to perform a deeper dive investigation.

For more information, see the *NetWitness Investigate User Guide*. For troubleshooting information with the Investigate > Events link see the *Alerting with ESA Correlation Rules User Guide*.

Pivot to the Hosts or Files View

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

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

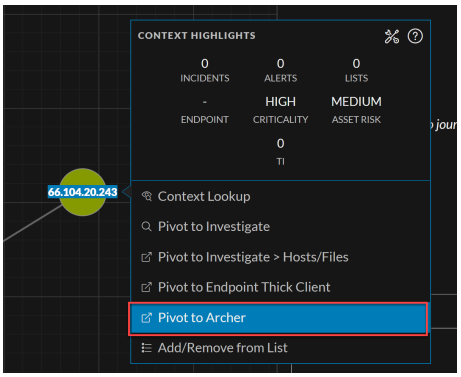
1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **Actions** section of the tooltip, select **Pivot to Endpoint Thick Client**.
   The NetWitness Endpoint thick client application opens outside of your web browser.

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

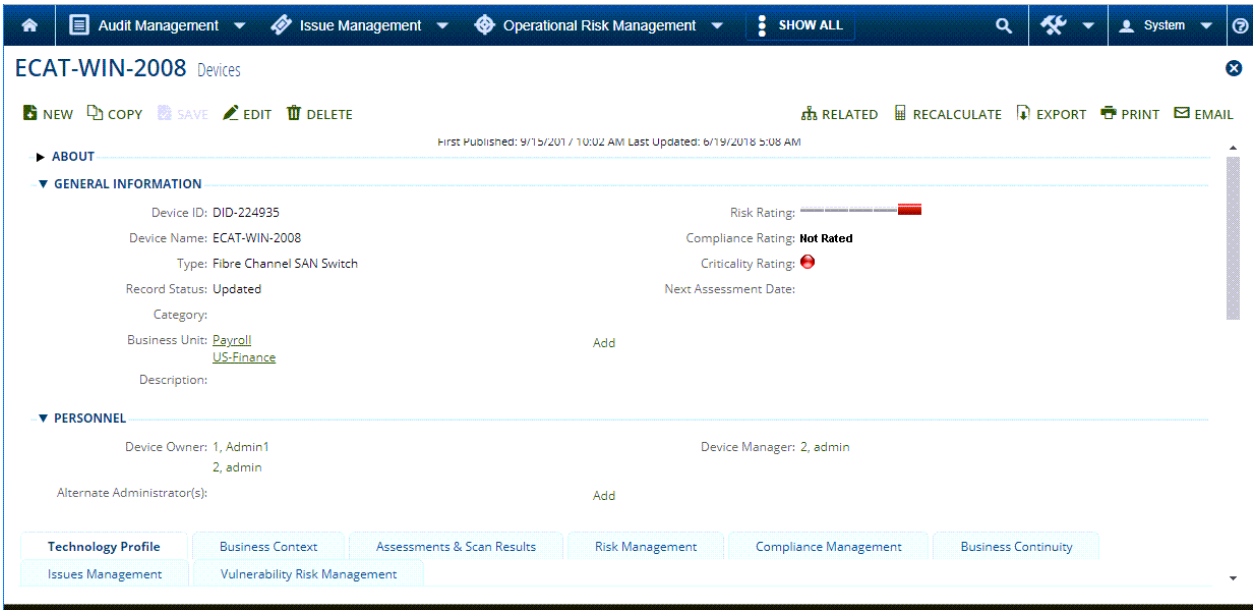
Pivot to Archer

For viewing more details about a device in 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, left or right click 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.



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 Archer configuration is enabled and configured properly.

For more information, see the *NetWitness 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 NetWitness Version 11.2 and later, you can change the assignee, category, and priority when you create an incident manually from alerts.

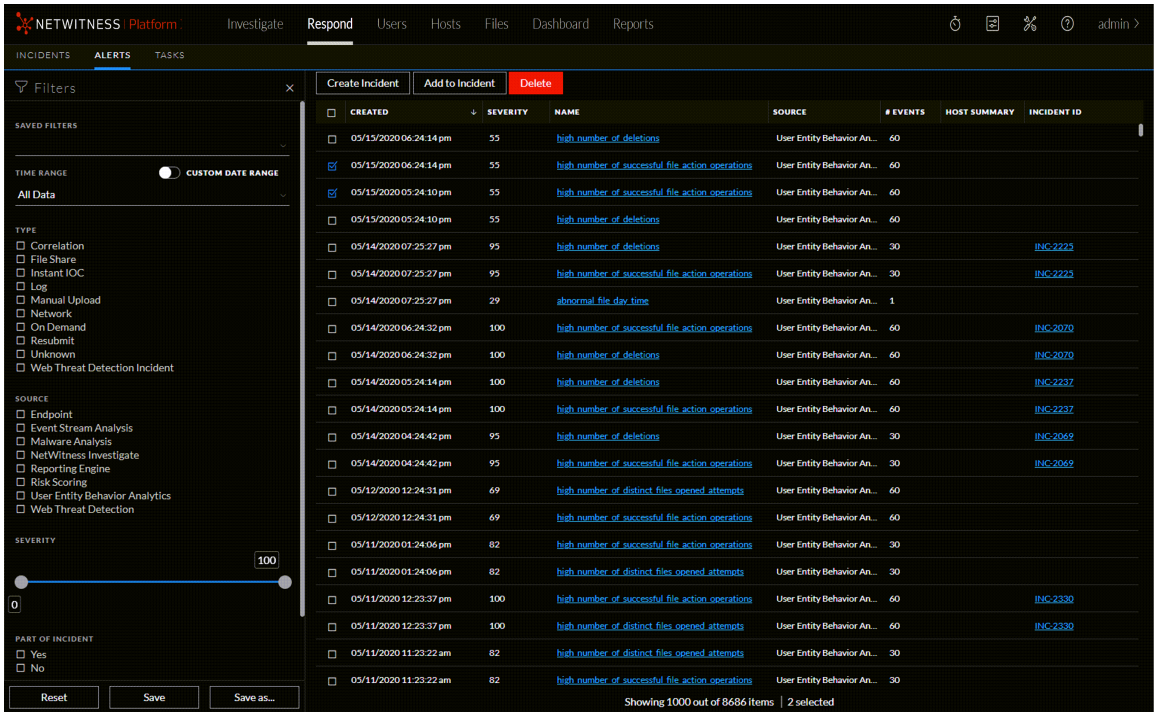
In NetWitness Version 11.1, incidents created manually from alerts default to Low priority, but you can change the priority after you create it. You cannot add categories to manually created incidents in version 11.1.

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:

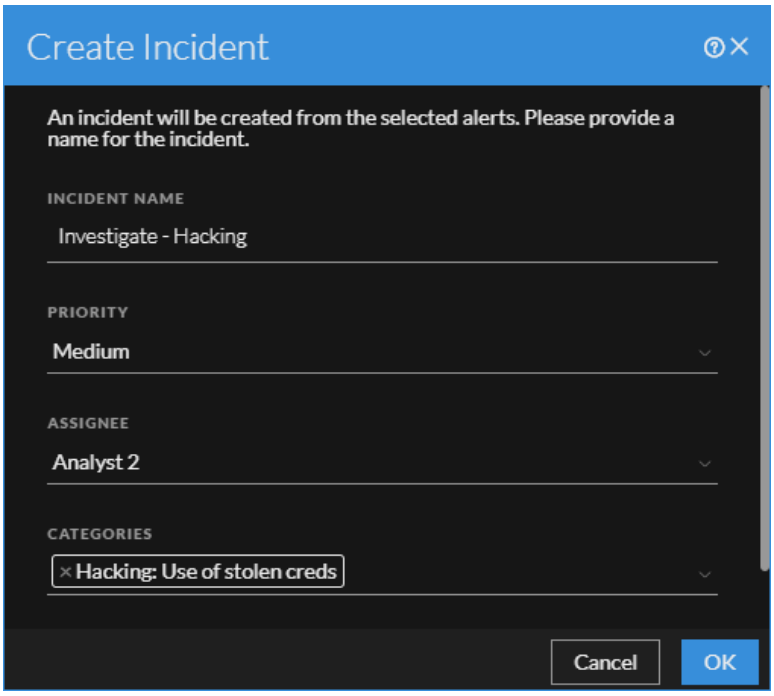
1. Go to **Respond** > **Alerts**.
2. Select one or more alerts in the Alerts List.

   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 Incidents** as **No** in the Filters panel.



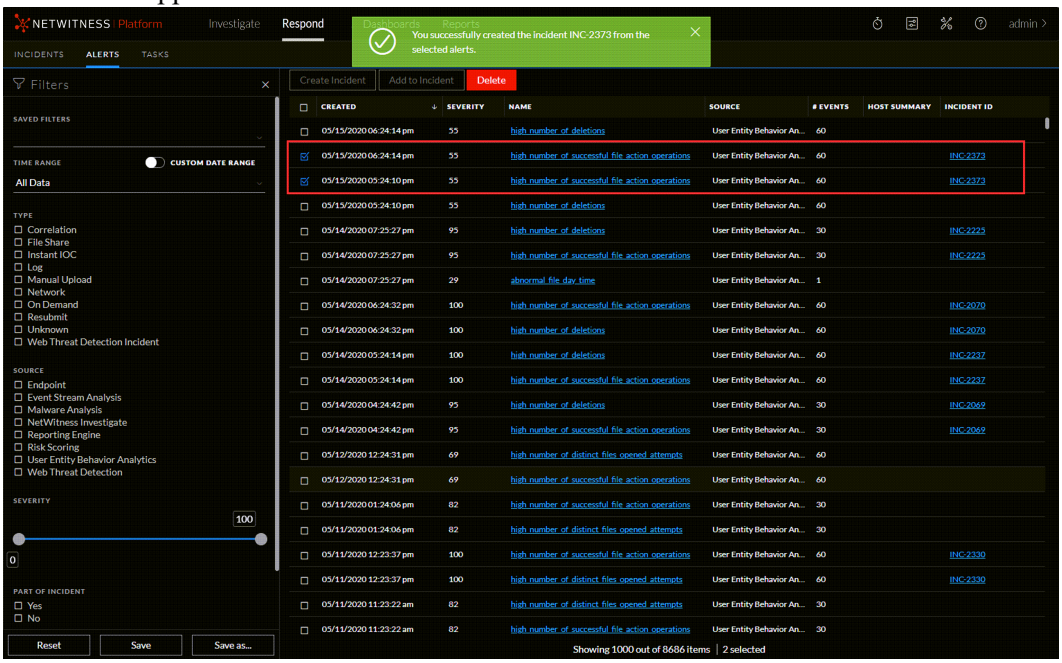
3. Click **Create Incident**.

   The **Create Incident** dialog is displayed.

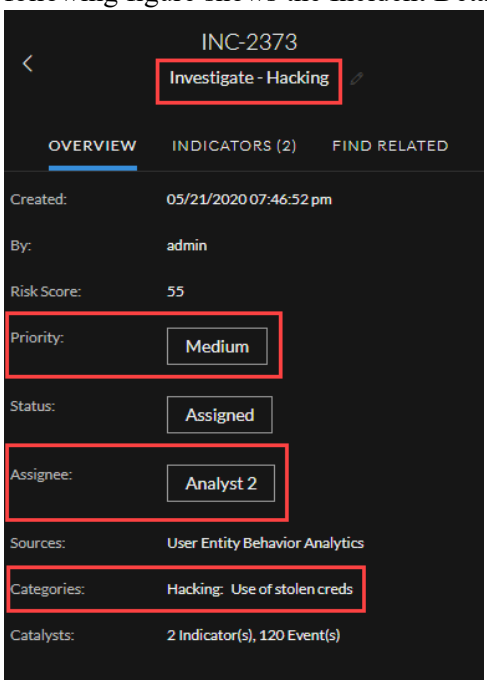


4. In the **Incident Name** field, type a name to identify the incident. For example, Investigate - Hacking.
5. In the **Priority** field, select a priority for the incident. The priority defaults to Low.
6. (Optional) If you are ready to assign the incident, in the **Assignee** field, select a specific 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.



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.



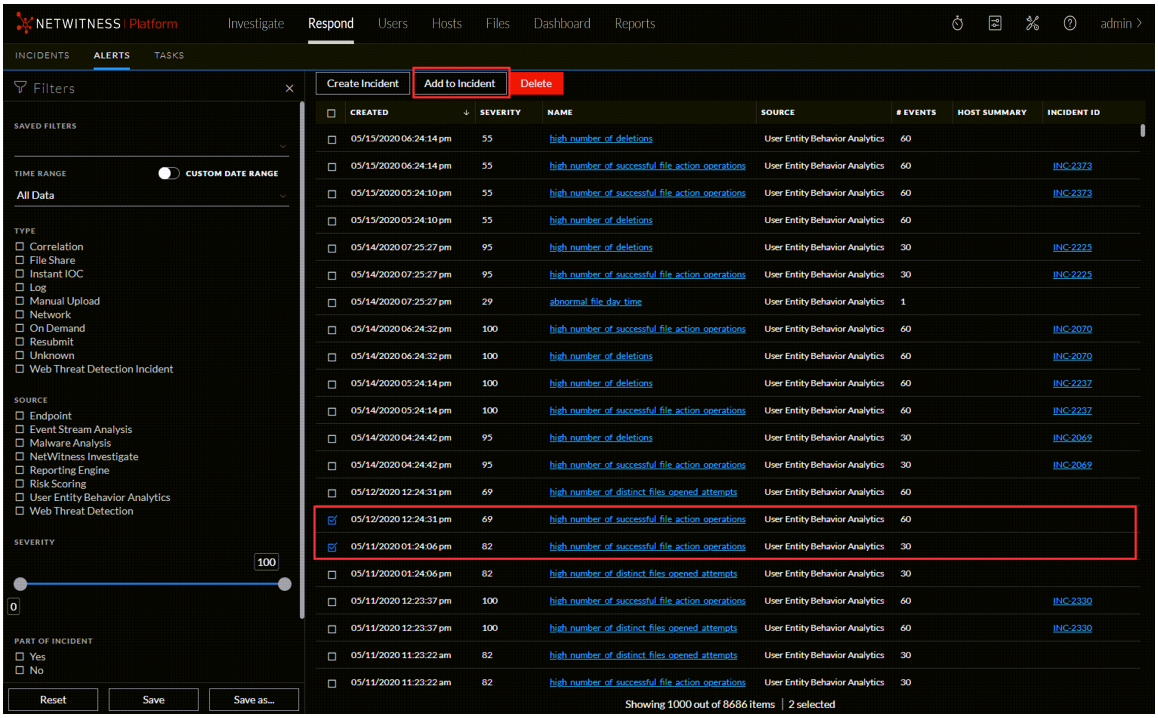
Add Alerts to an Incident

Note: This option is available in NetWitness Version 11.1 and later.

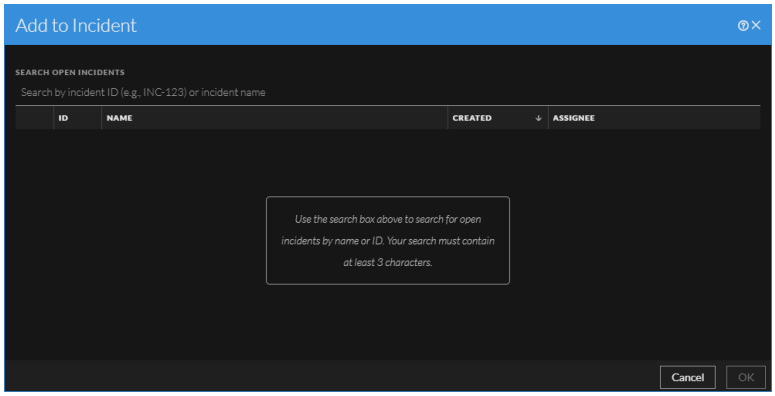
If you have alerts that fit a particular existing incident, you do not have to create a new incident. Instead, you can add alerts to that incident from the Alerts List view. The alerts that you select cannot be part of another incident.

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**.

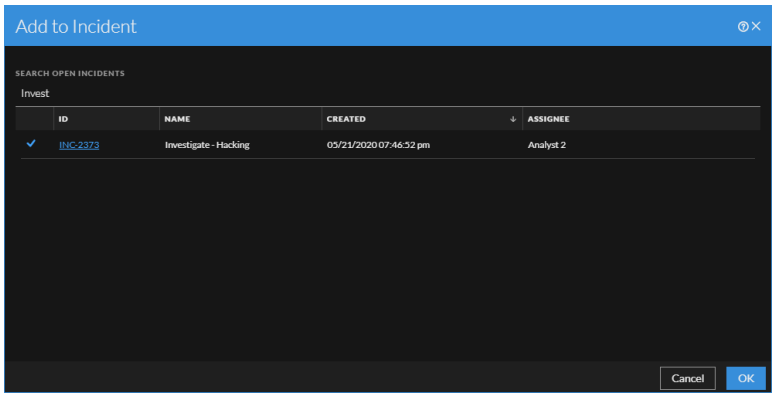
   Note: Selecting alerts that do not have incident IDs enables the **Add to Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **Part of Incident** as **No** in the Filters panel.



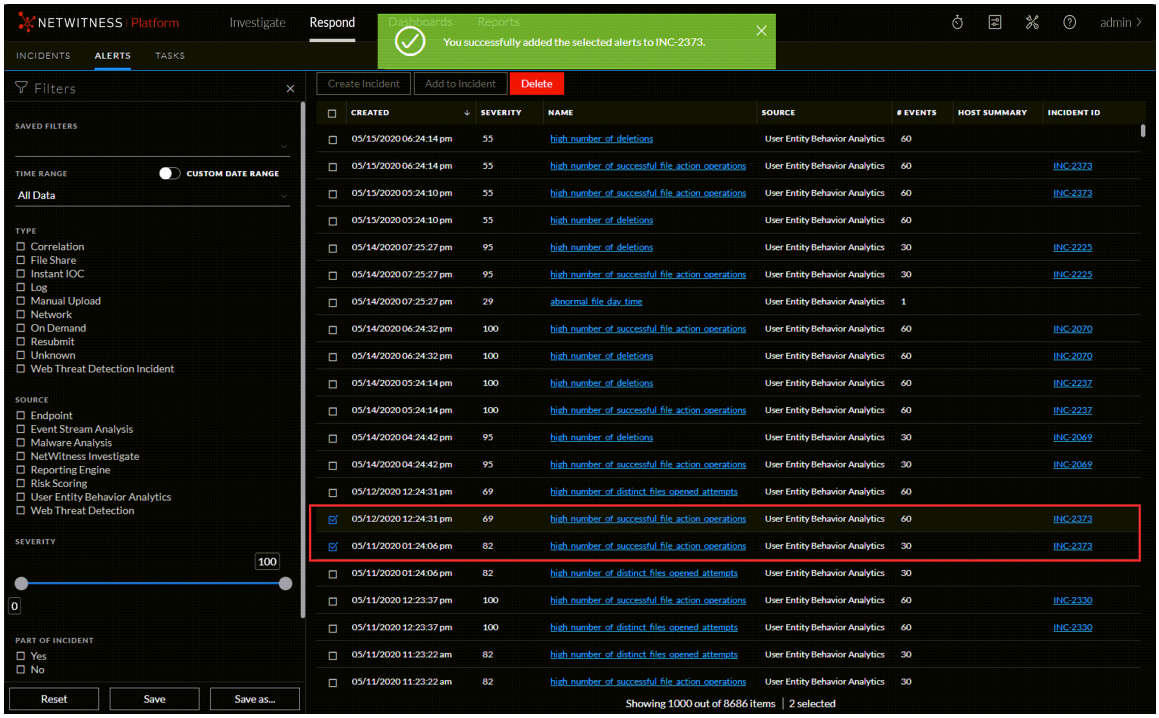
3. In the **Add to Incident** dialog, type at least three characters in the **Search** field to search for the incident by **Name** or **Incident ID**.



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



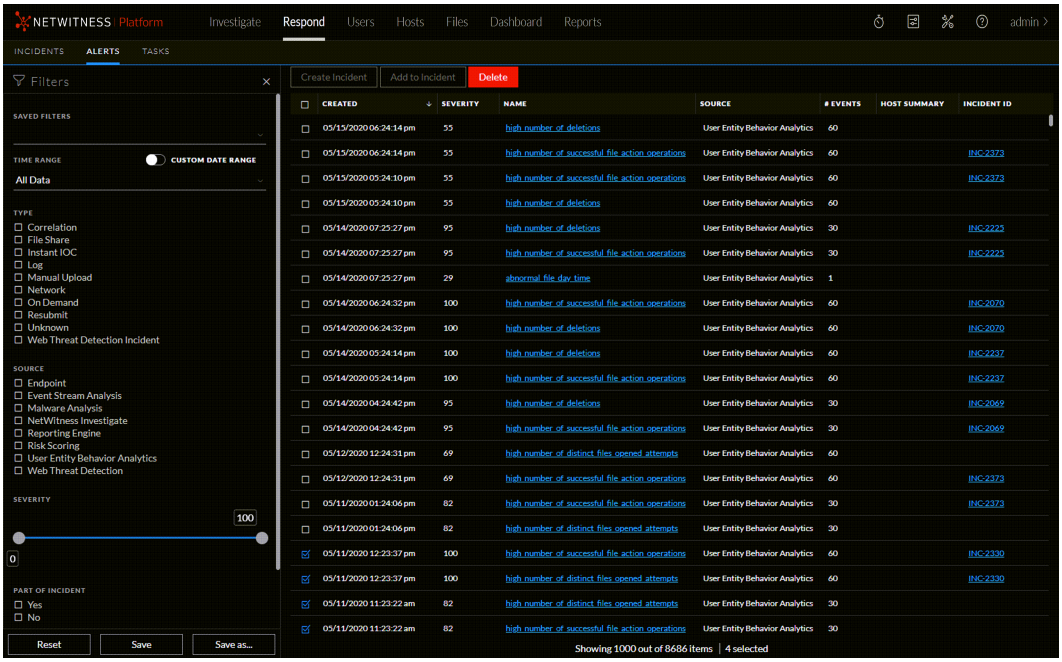
The selected alert or alerts are now part of the selected incident and will have that incident ID.



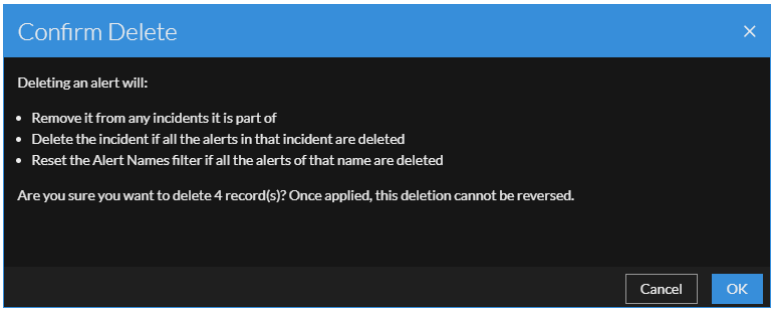
Delete Alerts

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

1. Go to **Respond > Alerts**.
   The Alerts List view displays a list of all NetWitness alerts.
2. In the Alerts list, select the alerts that you want to delete and click **Delete**.



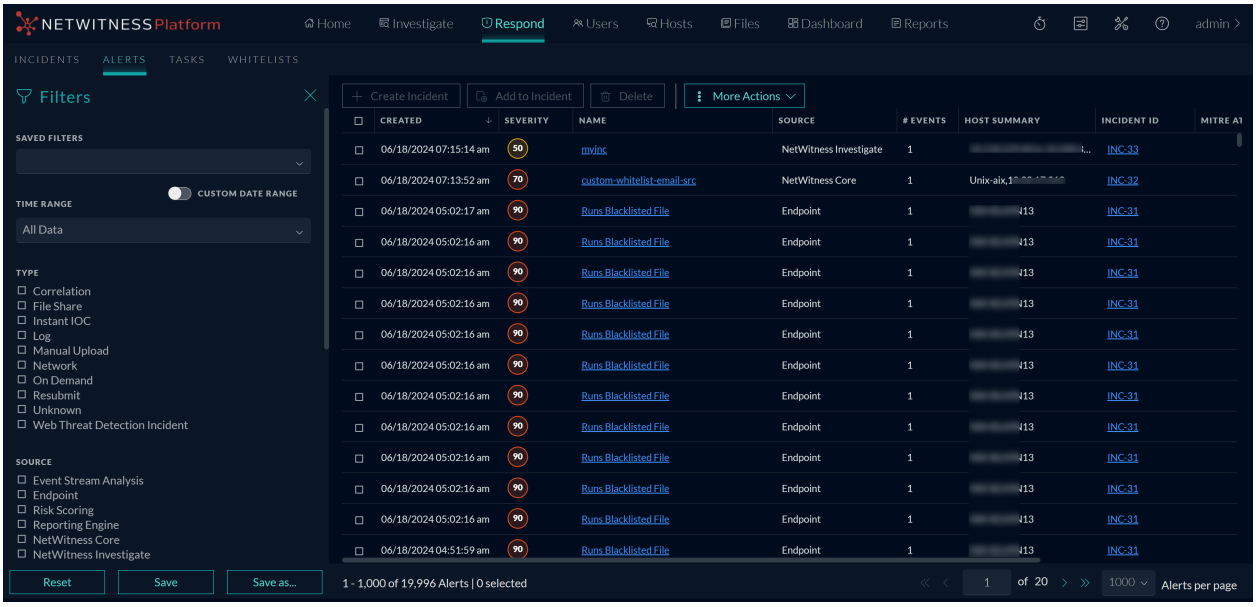
   If you do not have permission to delete alerts, you will not see the Delete button.
3. Confirm that you want to delete the alerts and click **OK**.



   The alerts are deleted from NetWitness. 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.

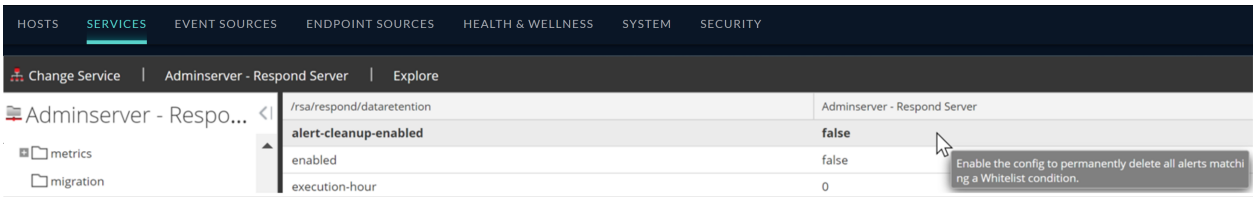
Whitelist Alerts

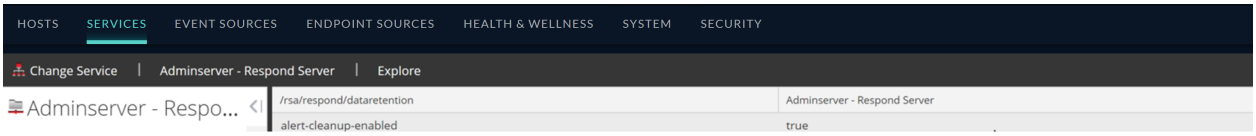
The **Whitelist Alert** feature allows you to whitelist the unwanted and recurring non-suspicious Endpoint alerts triggered in the **Respond** > **Alerts** view.



With this feature, you can select entities (meta part of the alerts) and define the Whitelist condition to avoid triggering unwanted alerts for the required entities. Administrators can permanently delete the existing alerts matched with the Whitelist condition by enabling the Config in the **Services** > **Respond Server** > **Explore** view.

Note: By default, the Config is disabled in the **Services** > **Respond Server** > **Explore** view (the `alert-cleanup-enabled` parameter is set to **false**). To enable the config, you must set the `alert-cleanup-enabled` parameter to **true** in **Services** > **Respond Server** > **Explore** view. Refer to the following figures.



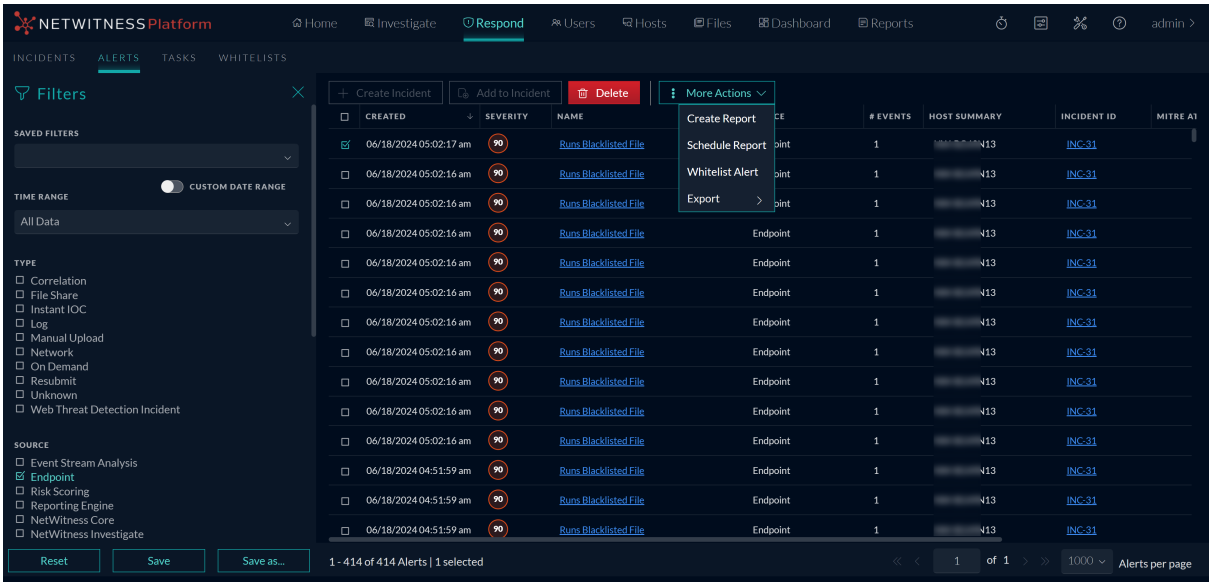


Note:
- When you enable the config, the existing alerts matched with the Whitelist condition still continue to exist over a period of time before they are permanently deleted. Once deleted, the alerts cannot be reversed to the selected entities.
- You can select only one alert at a time for whitelisting.

Note: NetWitness 12.5 extended the Whitelist feature to Event Stream Analysis and NetWitness Core. Now, you can whitelist unwanted and recurring non-suspicious alerts for these services.

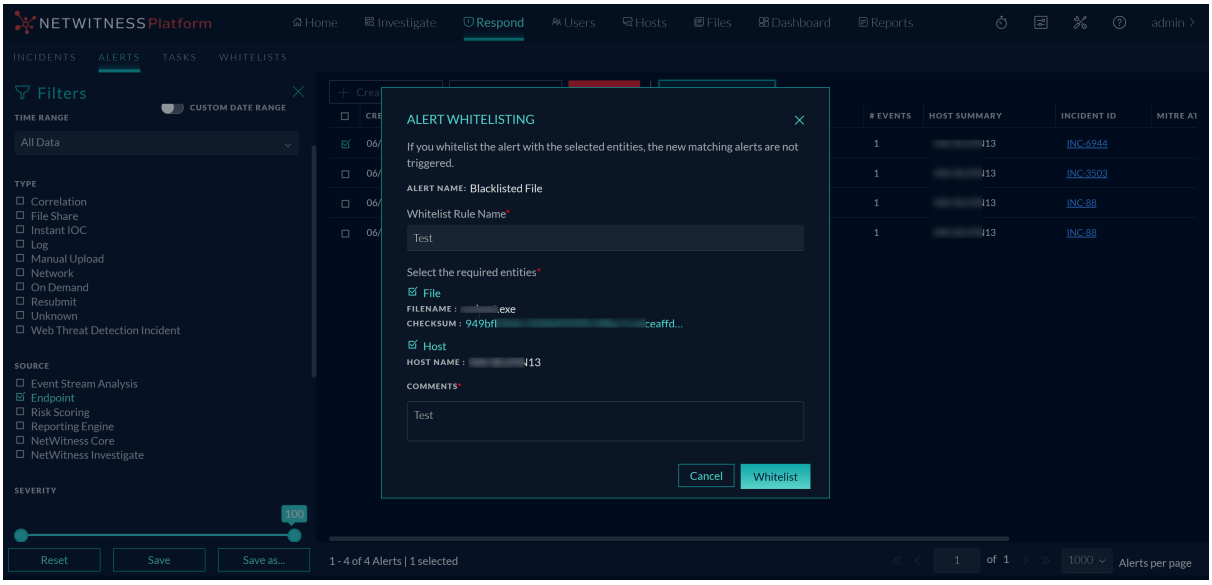
To Whitelist an Endpoint Alert

1. Go to **Respond** > **Alerts**. The **Alerts** view is displayed.
2. Select an alert and click **More Actions** > **Whitelist Alert**.



3. Enter the name of the Whitelist and select the required entities.

Note: Note: The entities displayed depend on the entities present on the selected Endpoint Alert. You must select at least one of the entities to apply to the Whitelist.



4. Specify the reason for whitelisting in the **Comments** section.

5. Click **Whitelist**.

   The **Confirm Alert Whitelist** confirmation dialog is displayed.

6. Click **Confirm Whitelist**.

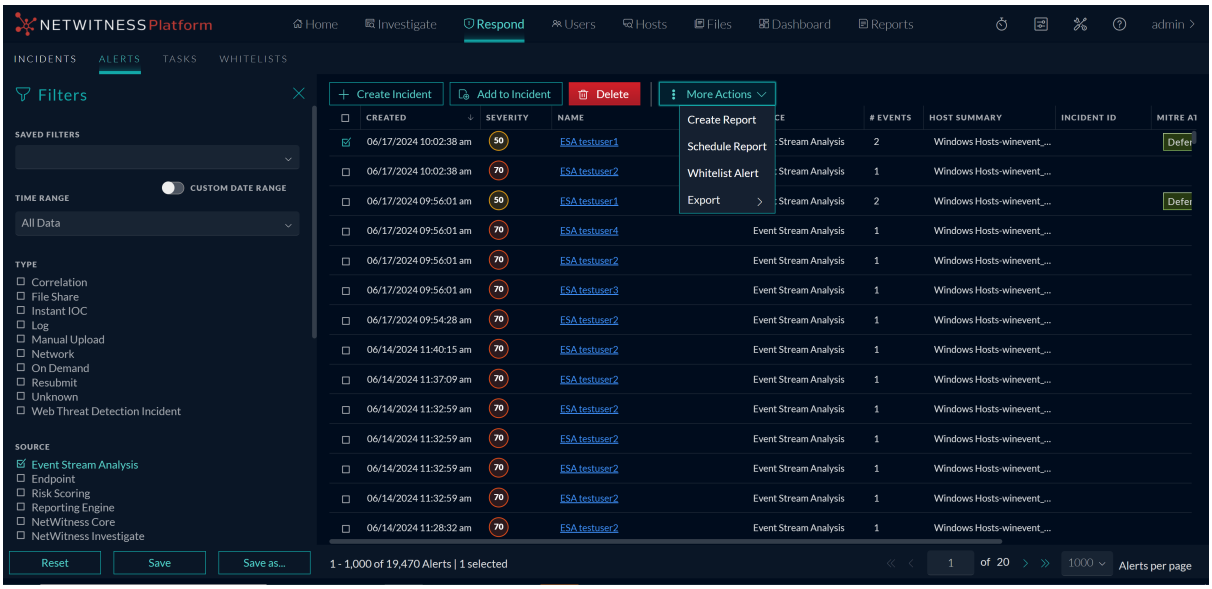
Meta Keys Supported

The following table shows the meta keys supported for Endpoint alert whitelisting:

Elements	Meta Keys
Source	`user.src`
Target	`user.dst`
Filename	`filename, filename.src, filename.dst`
Hostname	`alias.host, host.dst, host.src, device.host`

To Whitelist an Event Stream Analysis Alert (From NetWitness 12.5)

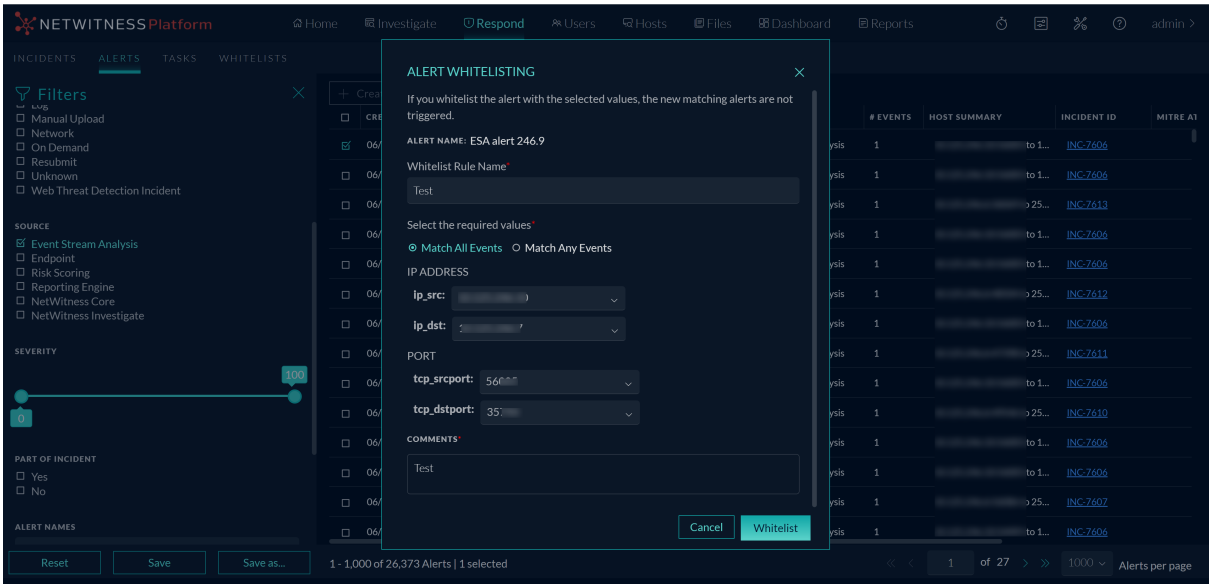
1. Go to **Respond > Alerts**.
2. Select the **Event Stream Analysis** Alert and click **More Actions > Whitelist Alert**.



3. Enter the name of the Whitelist and select the required entities.

Note: The entities displayed depend on the entities present on the selected ESA Alert. You must select atleast one of the entities to apply the Whitelist.

Note: In Event Stream Analysis Alert, you have the option to select either “Match All Events” or “Match Any Events”. Selecting “Match All Events” will Whitelist the Alerts only if the selected entities are present across all the events of that alert. Selecting “Match Any Events” will Whitelist the Alerts if the selected entities are present in any of the events of that alert. that alert.



4. Specify the reason for whitelisting in the **Comments** section.
5. Click **Whitelist**.

   The **Confirm Alert Whitelisting** confirmation dialog is displayed.

6. Click **Confirm Whitelist**.

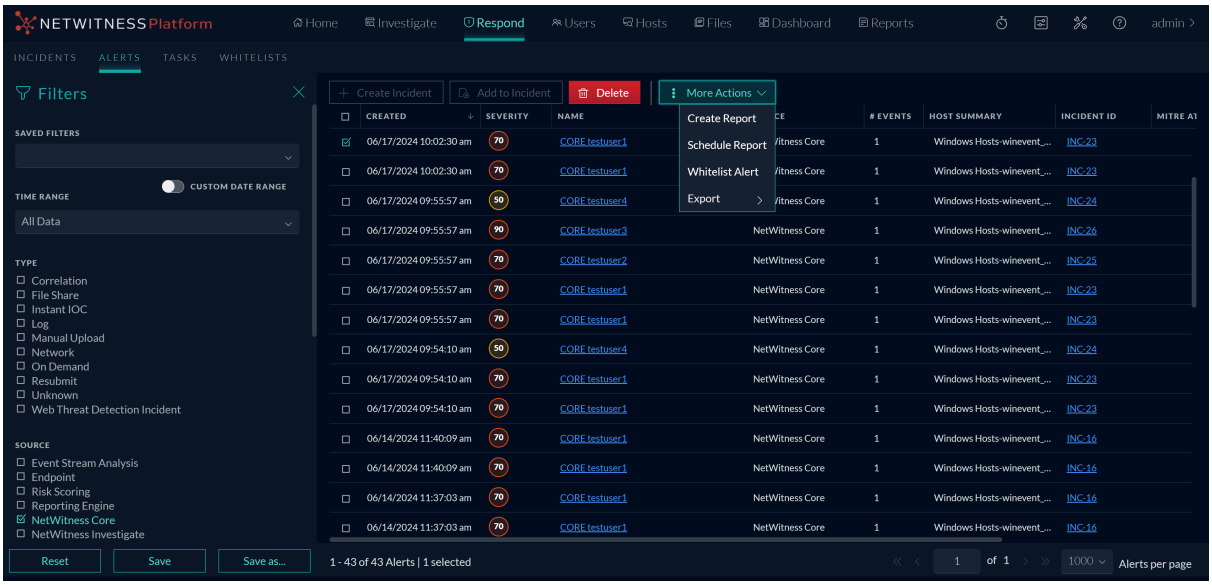
Meta Keys Supported

The following table shows the meta keys supported for ESA alert whitelisting:

Elements	Meta Keys
IP	`alias.ip, ip.src, ip.dst, forward.ip, device.ip`
Port	`tcp_srcport, udp_srcport, tcp_dstport, udp_dstport`
Filename	`filename, filename.src, filename.dst`
Action	`action`
Hostname	`alias.host, host.dst, host.src, device.host`

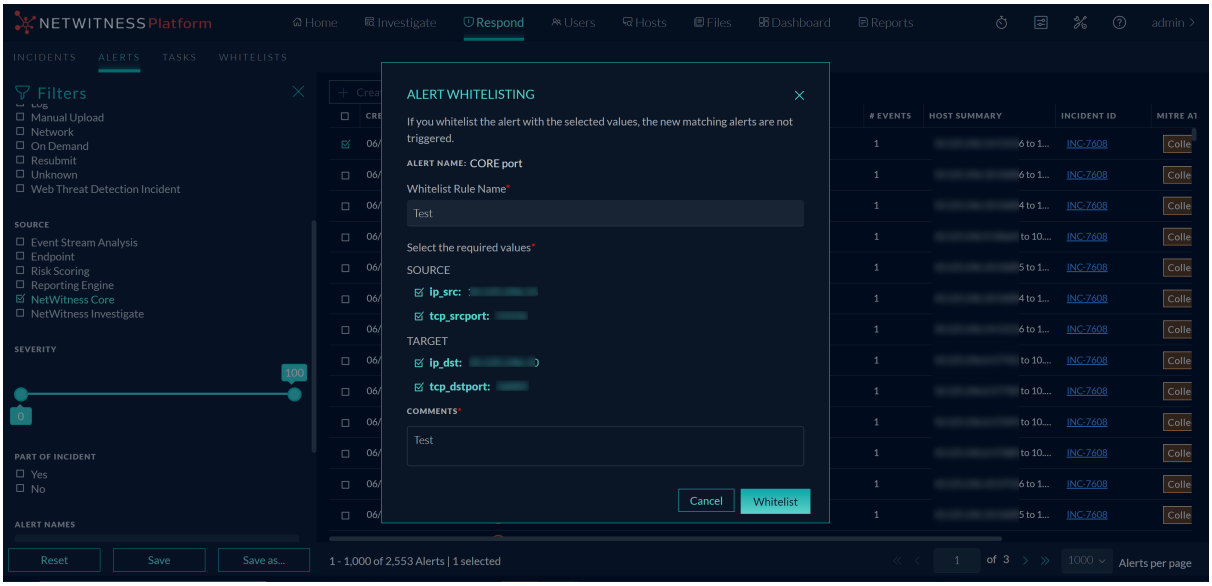
To Whitelist a NetWitness Core Alert (From NetWitness 12.5)

1. Go to **Respond > Alerts**.
2. Select the **NetWitness Core** Alert and click **More Actions > Whitelist Alert**.



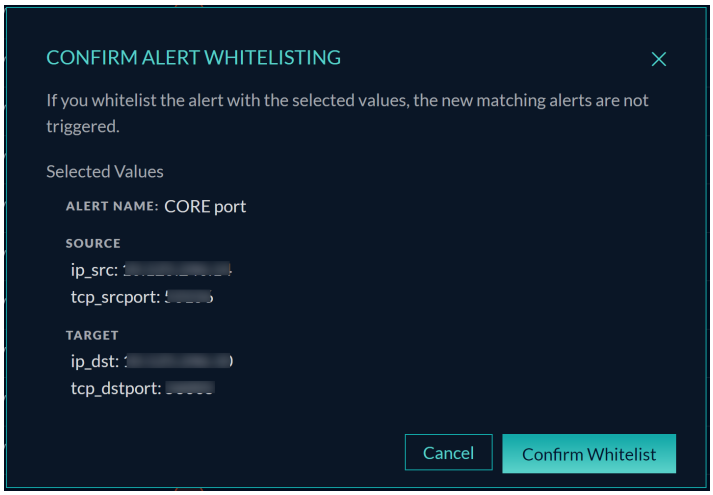
3. Enter the name of the Whitelist and select the required entities.

   The entities displayed depend on the entities present on the selected NetWitness Core Alert. You must select atleast one of the entities to apply the Whitelist.



4. Specify the reason for whitelisting in the **Comments** section.
5. Click **Whitelist**.

   The **Confirm Alert Whitelisting** confirmation dialog is displayed.



6. Click **Confirm Whitelist**.

Meta Keys Supported

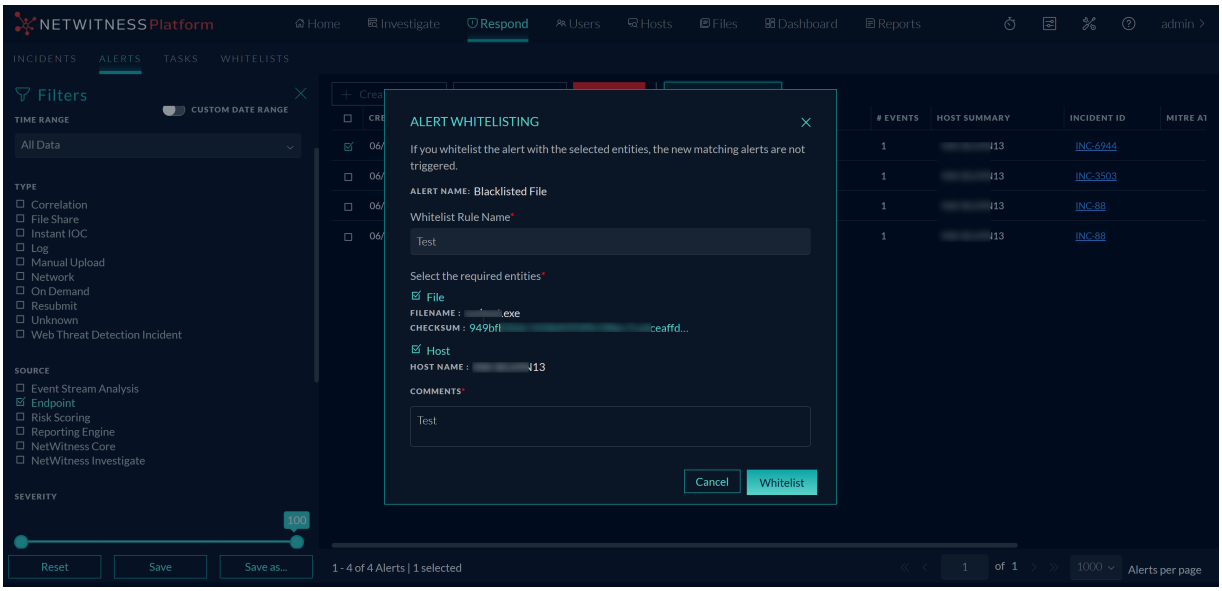
The following table shows the meta keys supported for NetWitness Core Alert whitelisting:

Elements	Meta Keys
Source	`host.src, ip.src, tcp_srcport, udp_srcport, user.src`
Target	`host.dst, ip.dst, tcp_dstport, udp_dstport, user.dst`
Domain	`domain, domain.src, domain.dst, alias.host, device.host`

Use Case: Unwanted Endpoint Alerts Triggering in the Respond service

John, an analyst, logs in to the NetWitness Platform and clicks **Respond** > **Alerts**. While investigating the alerts in the Respond **Alerts** view, John notices that a few alerts displayed in the UI are not suspicious. Analyst selects a non-suspicious alert and clicks the **Whitelist Alert** tab under **More Actions** in the toolbar. Once the **Alert Whitelisting** confirmation window is displayed, John performs the following:

- Enters the name of the Whitelist.
- Selects the entities **File**, **Host** and **User** to stop triggering the new matching alerts for the particular file **xxxx.exe** and the host **Windows**.



- Specifies the reason for whitelisting the alert in the **Comments** section and clicks **Whitelist**.
- Once the **Confirm Whitelist** confirmation window is displayed, John clicks **Confirm Whitelist**.

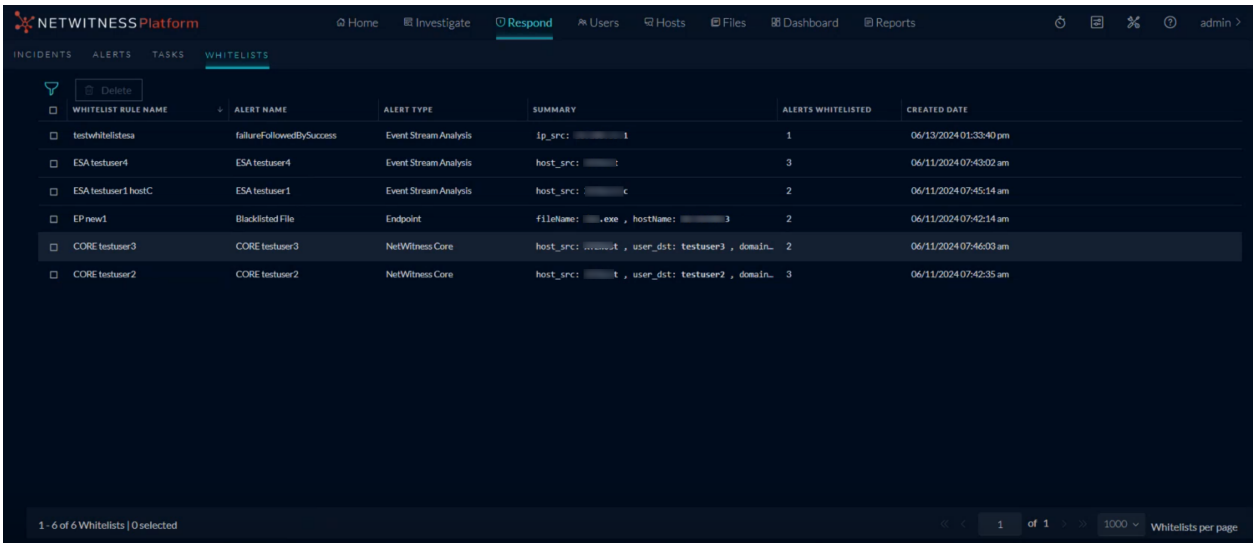
After whitelisting the selected alert, John selects another non-suspicious alert in the Respond Alerts view for whitelisting. This time, John enables the config in the **Services** > **Respond Server** > **Explore** view to permanently delete the existing alerts matched with the Whitelist condition. Later, John selects the entities **User**, **Host**, and **File** in the **Alert Whitelisting** confirmation window to stop triggering the new matching alerts for the selected entities.

Note: Upon enabling the config and then whitelisting the alert for the selected entities **User**, **Host**, and **File**, John finds that the risk score of the entities **File** and **Host** is affected. This is due to the permanent deletion of the existing alerts matched with the Whitelist condition after enabling the config.

Note: You can make similar Alert Whitelisting to Event Stream Analysis and NetWitness Core alerts.

Whitelists List View

The Whitelists List view displays the list of all the Endpoint, ESA, NetWitness Core, and Insight Whitelists with the Whitelist Rule Name, Alert Name, Alert Type, Summary, Alerts Whitelisted, and the Created Date associated with the respective Whitelisted Alerts. The view consists of a Filters panel, Whitelists List, and the Whitelist Overview.



Whitelists List

The Whitelists List displays all the Whitelists in the NetWitness Platform. You can filter this list to view only the Whitelists of interest.

The following table describes the columns in the Whitelists List.

Columns	Description
Whitelist Rule Name	Displays the name of the Whitelist you provided during the whitelisting of the selected alert.
Alert Name	Displays the rule name associated with the whitelisted alert.
Alert Type	Displays the alert type: ESA, Endpoint, and NetWitness Core.
Summary	Displays the details of the entities selected during the whitelisting of the selected alert. For Example: **File name: cmd.exe, Host name: win34.**
Alerts Whitelisted	Displays the number of number of alerts suppressed after the creation of Whitelist.
Created Date	Displays the Whitelist creation date and time.

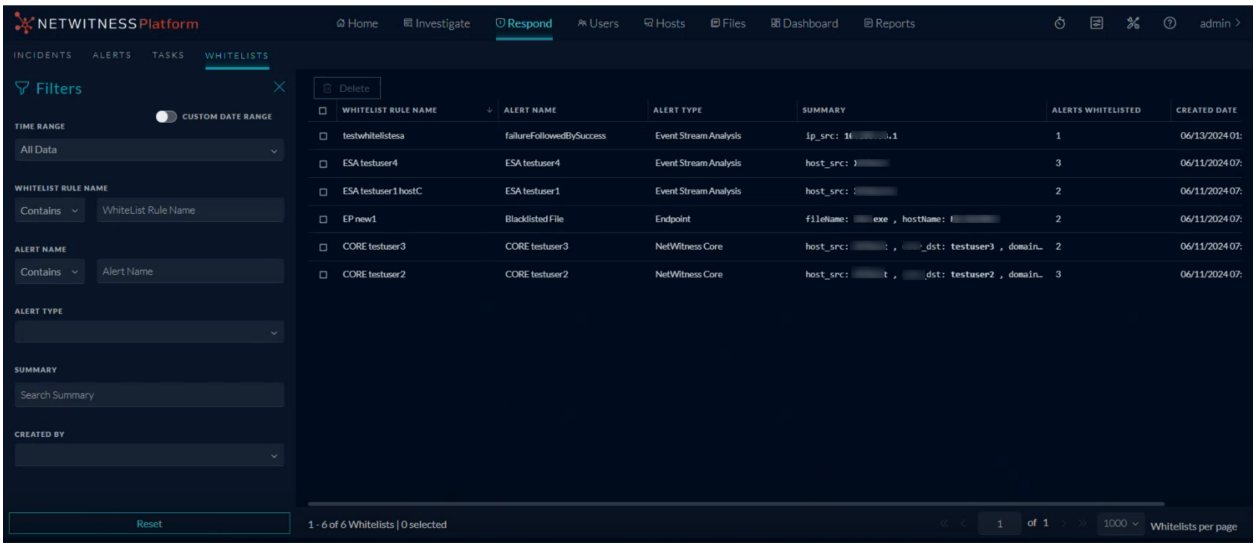
Filters Panel

You can filter the Whitelists based on the following parameters.

- Time Range
- Whitelist Rule Name
- Alert Name

- Alert Type
- Summary
- Created By

Click **Reset** to remove the filters applied.

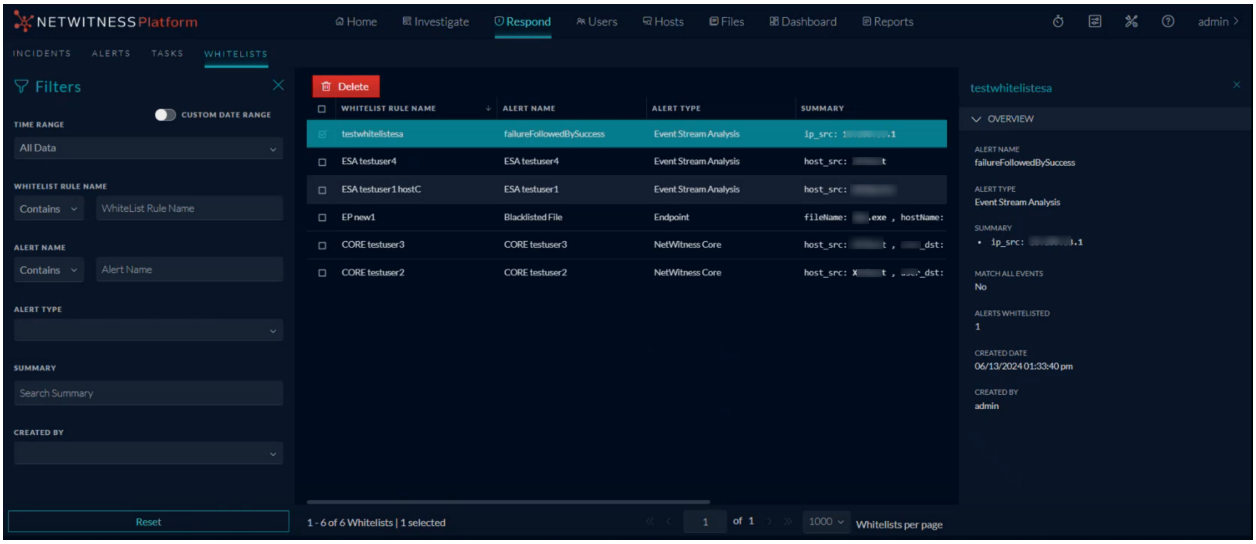


The following table lists all the fields displayed in the Whitelists List view Filters panel.

Fields	Description
Time Range	Allows you to select the required time duration and view the Whitelists created in the time duration selected. **Note:** Turn On the **Custom Date Range** Toggle to select a custom date range of your choice.
Whitelist Rule Name	Allows you to enter the name of required Whitelist.
Alert Name	Allows you to enter the name of the rule associated with the Whitelists created.
Alert Type	Allows you to select the alert type: ESA, Endpoint, NetWitness Core, and Insights.
Summary	Allows you to enter the complete value or a part of the value associated with the required Whitelist. For example: **cmd.exe** or **win34** or **analyst1**.
Created By	Allows you to filter the Whitelists on the basis of the user who created them.

Whitelist Overview

You can click on any whitelisted alert to view the overview on the right panel. All the selected entities will be displayed in the overview panel.

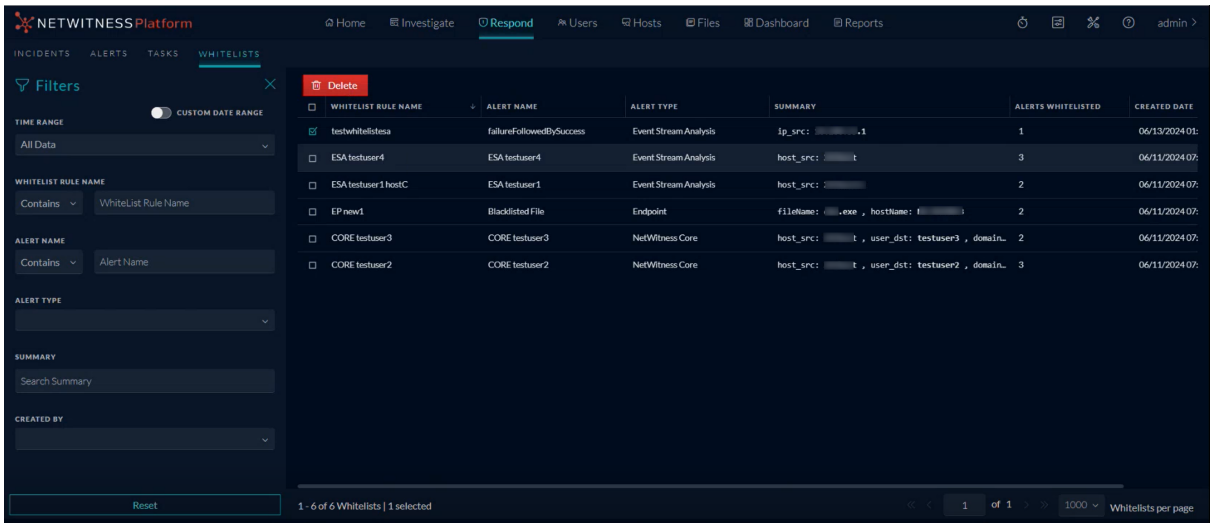


Delete the Whitelists

You can delete the Whitelists to start receiving the new matched alerts for the selected entities in the **Respond** > **Alerts** view. Once you delete the selected Whitelist, the new matching alerts are triggered only for the selected entities.

To delete the Whitelists

1. Go to **Respond** > **Whitelists**. The **Whitelists** view is displayed.
2. Select the Whitelist and click **Delete**.



The confirmation window is displayed.

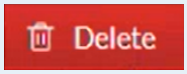
3. Click **Delete Whitelist**.

   The Whitelist is deleted.

Note:
- When you delete the Whitelists, only the new matching alerts are triggered. The whitelisted old alerts cannot be recovered for the selected entities.
- Analysts must have one of the following permissions to view the **Whitelists** tab in the **Respond** view:
  - **respond-server.alert.delete**
  - **respond-server.alert.read**
  - **respond-server.alert.manage**
  - **respond-server.alertrule.manage**
  - **respond-server.alertrule.read**
- Analysts must have the **respond-server.alert.read** permission to view the whitelists in **Respond** > **Whitelists** view and **respond-server.alert.manage** permission to delete the Whitelists.

Toolbar Actions

The table below lists the toolbar actions available in the Whitelists List view.

Option	Description
	Select this option and access the **Filters** panel to filter the required Whitelists.
	Select this option to delete the selected Whitelist.

Schedule Report Dialog from Respond View

The **Schedule Report** dialog enables you to create a schedule for the report. Reports can be scheduled hourly, daily, weekly, or monthly. In order to schedule a report at a specific time or on a daily, weekly, or monthly basis, you must configure the scheduling options on the Schedule report dialog.

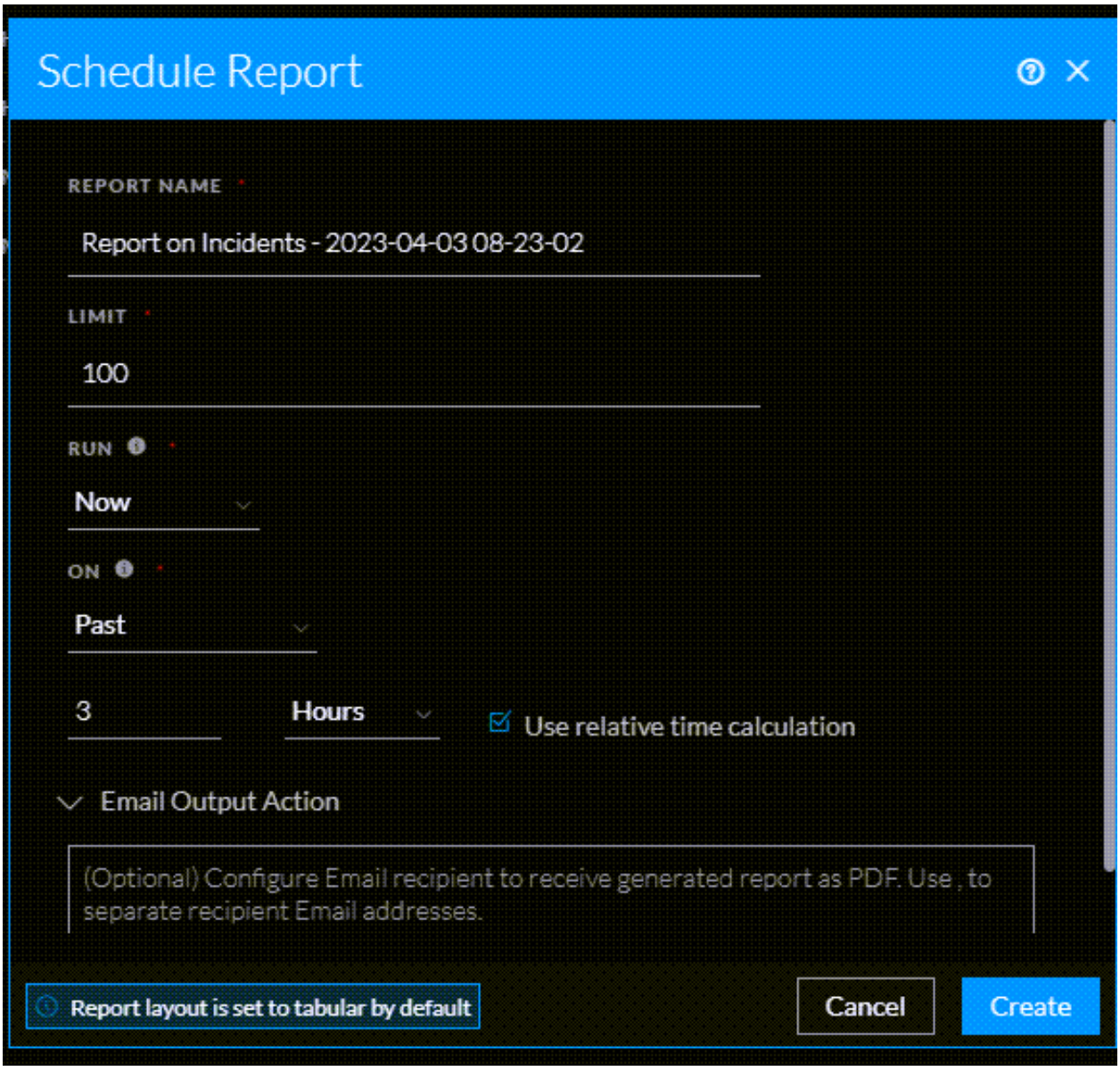
To access this dialog, Go to the **Respond** > **Incidents** view, add a query on the query search bar >  > **Schedule Report** from the toolbar.

What do you want to do?

User Role	I want to ...	Show me how
Administrator / Analysts	Schedule Report	Generate Reports from Respond View

Quick Look - Schedule Report Dialog

This is an example of the Schedule Report Dialog.



The following table describes the fields in the **Schedule Report Dialog** view.

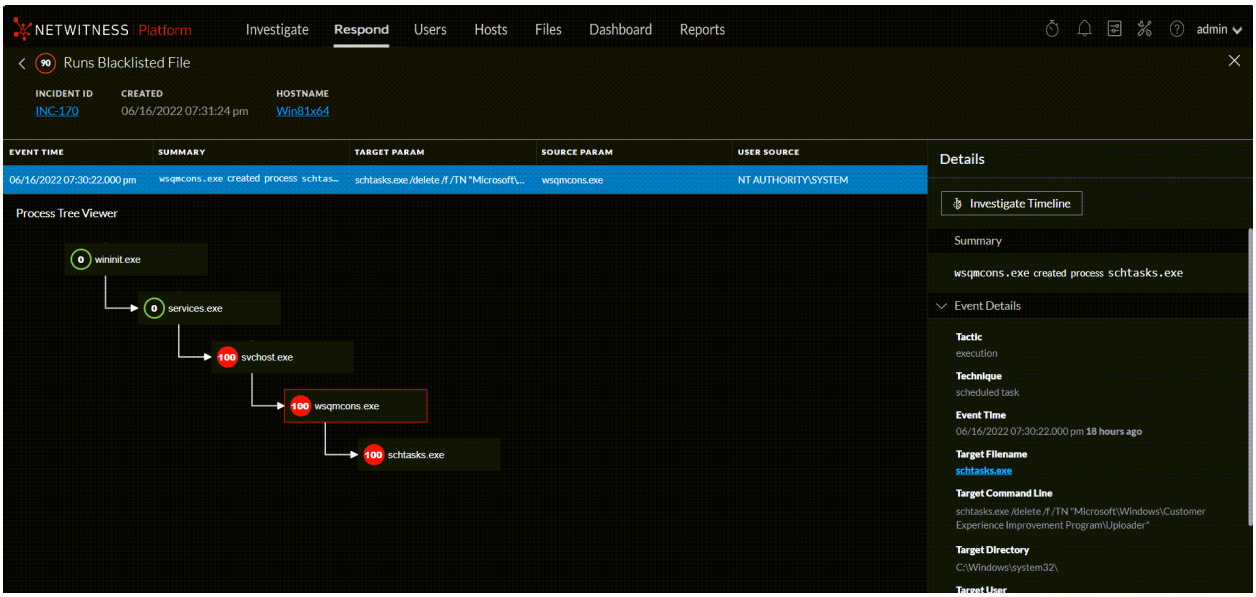
Feature	Description
Report Name	Specifies a name to identify the panel. For example, **Report on Incident - 2023-04-25 10-18-26**. You can provide a name that clearly identifies the nature of events that will be added to this report.

Feature	Description
Run	Time interval to use for running the scheduled job: • **Later**: Runs on specific date and time. • **Hourly**: Runs on a designated repeating interval. For example, if you schedule the report for 50 minutes, for every 50th minute, the report will be prepared. **Note:** A maximum of only 59 minutes can be selected. • **Daily**: Runs daily at a designated time. For example, if you schedule the report at 04:25, the report will be prepared at 04:25 AM every day. • **Monthly**: Runs on a monthly basis at a designated time and day of the month. For example, select 25 for the 25th day of the month. The report will be prepared on the 25th month of every month. **Note:** During the monthly report generation process, a message will appear if the day is greater than 28. This will notify the user that the report will be scheduled for the month containing that day.
ON	Set the frequency, duration, and time for running the report: • **Past**: You can schedule the report based on **Hours**, **Days**, **Weeks**, **Months**, and **Years**. • **Range(specific)**: You can schedule the report for a specific date and time range. **Note:** This field appears only if you select Later in the Run field. • **Range(generic)**: You can schedule the report for a generic date and time. **Note:** This field appears only if you select Later, Daily, Weekly, and Monthly in the Run field.
Use relative time calculation	The Use relative time calculation option is enabled by default, and it uses the relative time duration to schedule a report. For example, if you schedule a report to run over the past 1 hour –1h for the relative time, the time is exactly 1 hour from when the report is run. If the current time is 3 P.M., the events that occurred in the past 60 minutes or between 2 P.M. and 3 P.M. today.
Email Output Action	Specify email addresses to send the report to, separated by commas.
Create	Creates the report and closes the dialog. A message confirms that the report was scheduled successfully.
Cancel	Closes the dialog without applying changes.

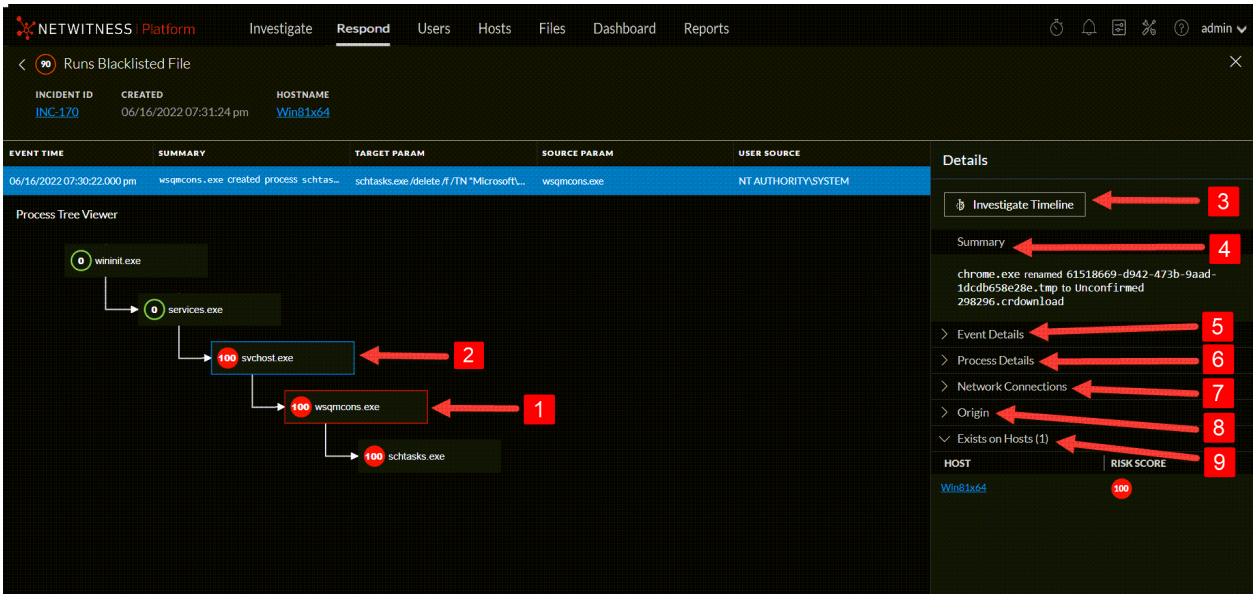
Review Endpoint Alerts using Process Tree

From version 12.0.0.0 and higher, the Alert details page for Endpoint alerts will show a process tree along with the details of Summary, Event details, Process details, etc.

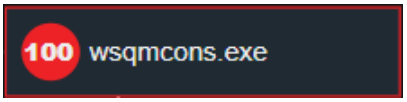
After you filter the Endpoint alerts in the Alerts List view, you can go to the Alert Details view for more detailed information on the Endpoint alerts, to determine the action required. An alert contains one or more events. In the Alert Details view for Endpoint alerts, you can view the alert details in the form of a process tree and additional event details, process details and much more on the right panel. The following figure shows an example of the Alert Details view for Endpoint alerts.



The process tree on the Alert Details view provides a complete picture about where the suspicious/malicious file originated including the path in the form of a process tree.



The **Details** panel on the right has more information for an alert than the Overview panel in the Alerts List view.



- The file that caused the alert is outlined in red.

- Selected file is outlined in blue.

1 - The file that caused the alert, and it is outlined in red. If you click on this file, the red outline will become blue to show it is selected.

2 - The file from which the suspicious/malicious file is originated.

3 - **Investigate Timeline** takes to the Investigate view for the selected alert.

4 - **Summary** shows a short description of the event.

5 - **Event Details** section provided a detailed information about the event that includes the Event Time, Target Filename, Tactic, Technique, Target User etc.

6 - **Process Details** section shows the Directory where the file is stored besides User name, Hash value, Risk score, Signature etc.

7 - **Network Connections** shows any network connection the selected file established since ten minutes before and till ten minutes after the alert triggered time. For example, if the alert was triggered at 16:00 hours, the network connections(if any)established by the selected file from 15:50 hours to 16:10 hours will be shown.

8 - **Origin** section shows how the selected file originated in the host.

9 - **Exists on Hosts** shows the list of hosts(with risk score) the selected file exists.

Process Details Section Values

Name	Description	Example
Tactic	Shows the tactic, as per MITRE ATT&CK frame work, this attempt falls under.	*execution*

Name	Description	Example
Technique	Shows the technique, as per MITRE ATT&CK frame work, this attempt falls under.	*masquerading*
Event Time	Shows the event occurred time.	*06/22/2022 10:14:28.000 am 8 hours ago*
Target Filename	Shows the name of file that is targeted. You can also view it in the process tree, next to the file that caused the alert.	*Unconfirmed 298296.crdownload*
Target Command Line	Shows the command line argument of the target file.	N/A
Target Directory	Shows the targeted directory.	*C:\Users\Administrator\Downloads*
Target User	Shows the user name through which the attempt was made.	*WIxxxxxx\Administrator*
Target Hash	Shows the hash value of the selected file.	*f214c48dc1daxxxx41d327c6bed1b52xxxx492573d85a305d8183eaa0222cc96*

Event Details Section Values

Value	Description	Example
File name	Shows the selected file name with extension	*iexplore.exe*
Command Line	Shows the command line name for the selected file	*IEXPLORE.EXE*
Directory	Shows the location of the selected file	*C:\Program Files\Internet Explorer*
User	Shows the user name	*WIxxxxxx\Administrator*

Hash	Shows the hash value of the selected file	*f214c48dc1daxxxx41d327c6bed1b52xxxx492573d85a305d8183eaa0222cc96*
Risk Score	Risk score of the selected file	*100*
Signature	Shows whether the selected file is signed or not	*microsoft,signed,valid*
Reputation Status	Shows the reputation of a file hash	*Suspicious*
File Status	Shows the file status for the selected file	*Blacklist*

Note: The process tree will be invisible if you drag it to the right end of the screen. Refresh the page to reload the process tree.

ESA Primary Disaster Recovery

NetWitness Platform allows Administrators to perform ESA DR failover in the event of a disaster or unplanned outage of the original active ESA Primary node. You can set up an ESA Primary StandBy Node and make it an active ESA Primary node during the failover process. For more information on how to perform the ESA DR failover, see NetWitness Deployment Guide for 12.5.

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.

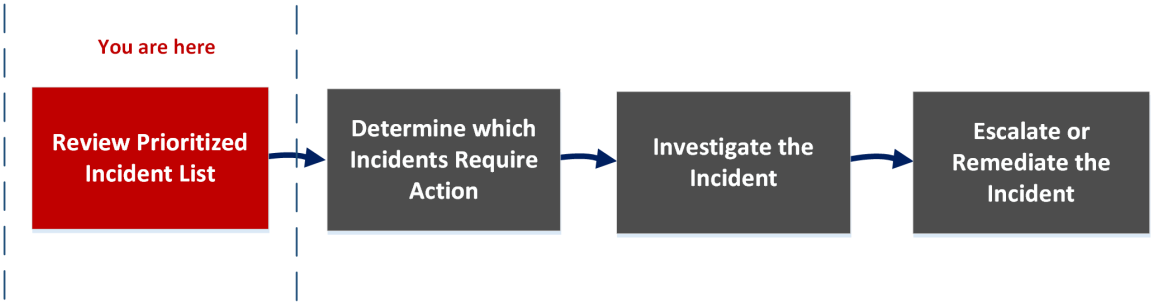
Topics

Incidents List View

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 or NetWitness Endpoint. 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.



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

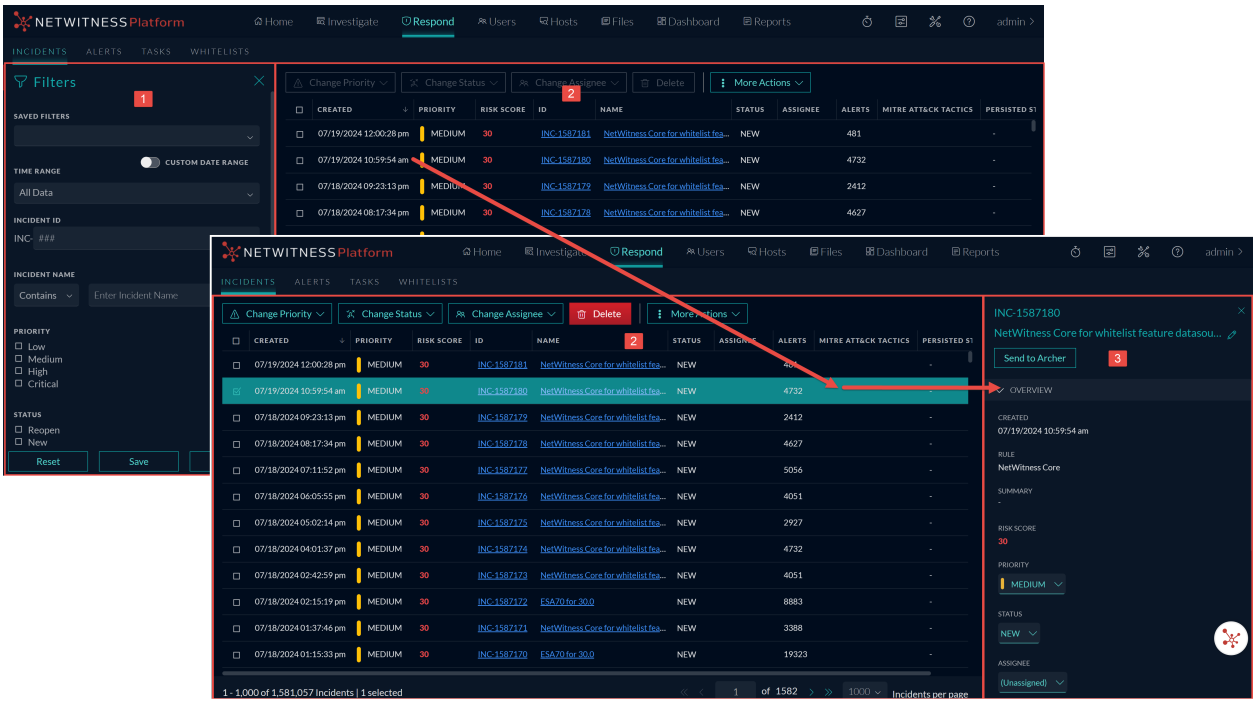
*You can complete these tasks here (that is, in the Incidents List view).

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.



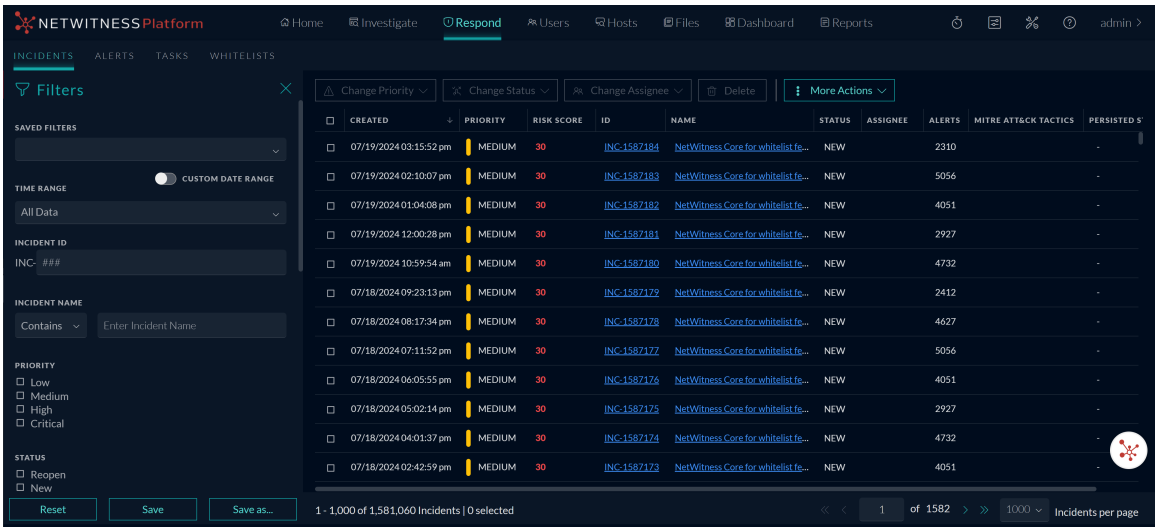
1 Filters Panel
2 Incidents List
3 Overview Panel

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

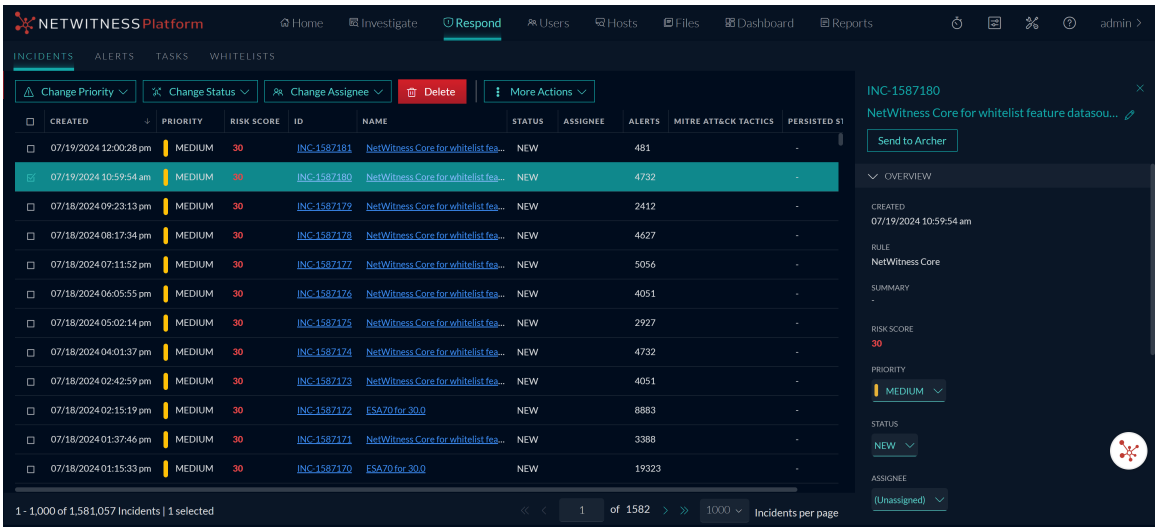
Incidents List View

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

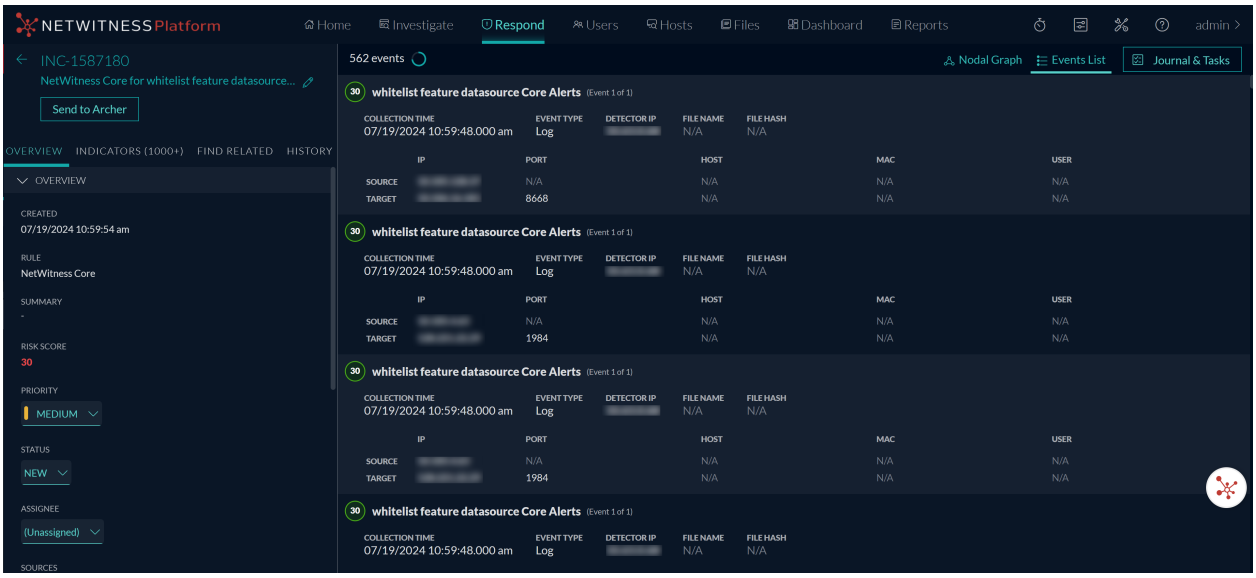
The following figure shows the Filter Panel on the left and the Incidents List on the right.



The following figure shows the incident Overview panel on the right.

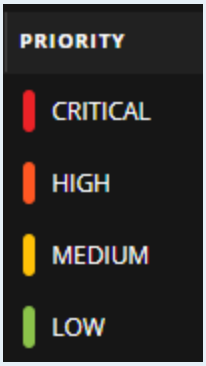


The following figure shows the incident Overview panel on clicking the Incident ID.



Incidents List

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

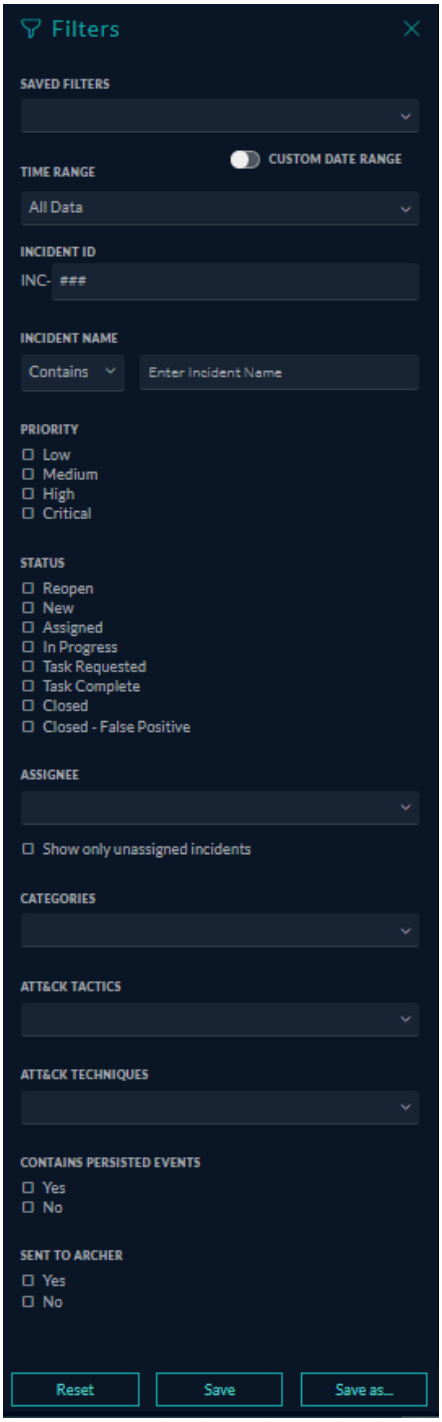
Column	Description
Created	Shows the creation date of the incident.
Priority	Shows the incident priority. Priority can be Critical, High, Medium, or Low. The Priority is color coded, where red indicates a **Critical** incident, orange represents a **High** risk incident, yellow indicates a **Medium**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

Column	Description
Name	Shows the incident name. The incident name is derived from the rule used to trigger the incident. Click the link to go to the Incident Details view for the selected incident.
Status	Shows the incident status. The status can be: Reopen, 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.
MITRE ATT&CK Tactics	Shows the particular Tactic associated with each Incident. For example: **Credential Access**. For more information on MITRE ATT&CK Tactics, see Use MITRE ATT&CK® Framework topic.
Persisted Status	Shows the persist status of the Incident. The status can be Complete, Partial, or None (-).

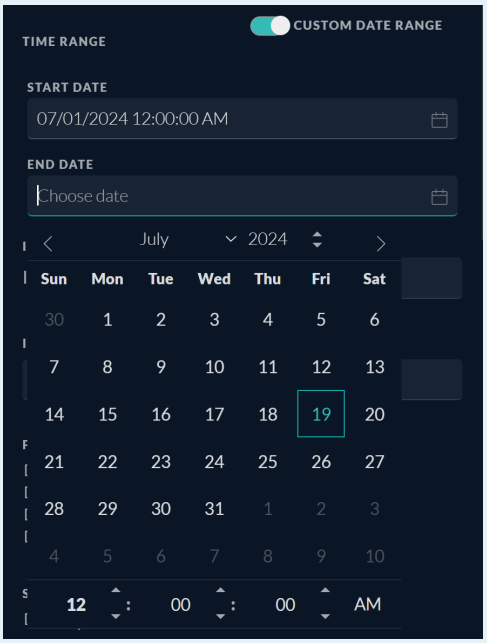
At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number of incidents selected. For example: **Showing 1000 out of 2517 items | 2 selected**. The maximum number of incidents that you can view at one time is 1,000.

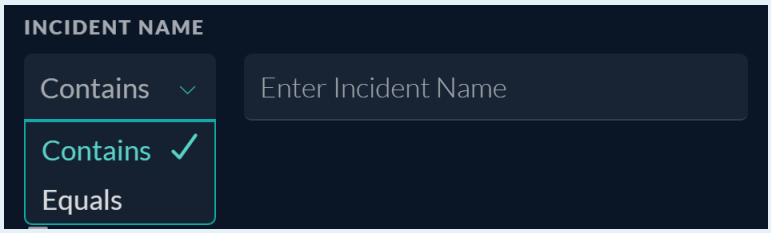
Incident Filters Panel

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



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

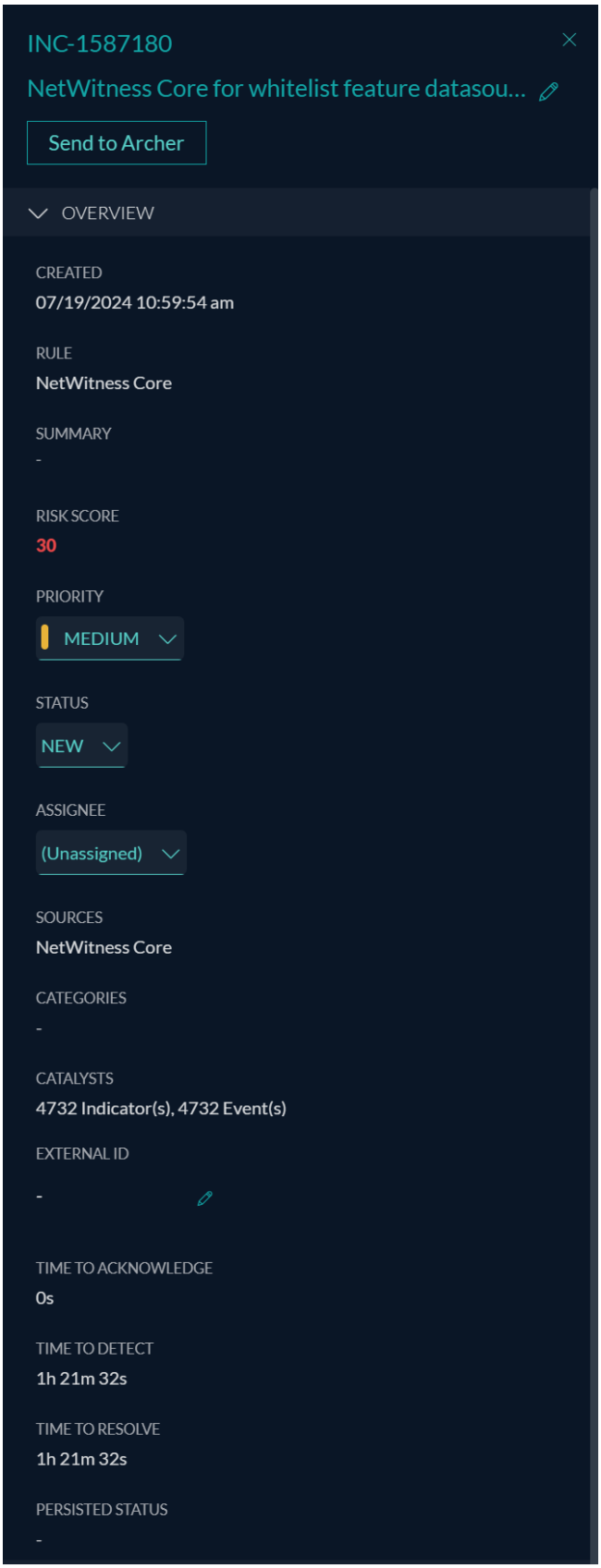
Option	Description
Saved Filters	You can select a saved filter to filter the incident list. Saved filters are global. You can save a filter for other analysts to use and you can use any saved filter. Saved filters are also available for use on the Springboard landing page. Filters used in the Springboard cannot be deleted. (This option is available in NetWitness Platform 11.5 and later.)
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.
Custom Date Range	You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar. 
Incident ID	Type the number of the incident that you would like to locate. For example, for INC-1050, type only the number "1050" to view the incident.

Option	Description
Incident Name	Enter the exact name of the Incident or a part of it to filter the list of required incidents. Select one of the following options to filter the list of required Incidents: • **Contains**: Select this option and enter the common term specified in the Incident names (of the required Incidents) to obtain a list of filtered Incidents in the Incidents List view. • **Equals**: Select this option and enter the exact name of the required Incident to obtain the filtered incident in the Incidents List view. 
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 NetWitness 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.
ATT&CK Tactics	Select the tactic associated with the incident.
ATT&CK Techniques	Select the technique associated with the incident.
Contains Persisted Events	Select a filter to view incidents based on the persisted events.
Sent to Archer	(In NetWitness Version 11.2 and later, if 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**.

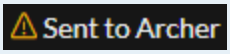
Option	Description
Reset	Removes your filter selections. If you reset filters on a saved filter, it takes you to the default empty filter.
Save	Saves the currently applied incidents filter or updates a saved filter. For a new filter, choose a unique name that contains 1-256 alphanumeric characters, underscores, or hyphens. (This option is available in NetWitness Platform 11.5 and later.)
Save As	Saves the currently applied incidents filter for future use. Choose a unique name that contains 1-256 alphanumeric characters, underscores, or hyphens. (This option is available in NetWitness Platform 11.5 and later.)

Incident 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.


INC-1587180
NetWitness Core for whitelist feature datasou...
Send to Archer
OVERVIEW
CREATED
07/19/2024 10:59:54 am
RULE
NetWitness Core
SUMMARY
-
RISK SCORE
30
PRIORITY
MEDIUM
STATUS
NEW
ASSIGNEE
(Unassigned)
SOURCES
NetWitness Core
CATEGORIES
-
CATALYSTS
4732 Indicator(s), 4732 Event(s)
EXTERNAL ID
-
TIME TO ACKNOWLEDGE
0s
TIME TO DETECT
1h 21m 32s
TIME TO RESOLVE
1h 21m 32s
PERSISTED STATUS
-

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

Field	Description
<Incident ID>	Displays the Incident ID.
Send to Archer / Sent to Archer	(In NetWitness Version 11.2 and later, if 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: • **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	Shows the name of the rule that created the incident or the name of the person who created the incident.
Summary	shows a short description of the incident.
Risk Score	Shows a value between 0 and 100 that indicates the risk of the incident as calculated by an algorithm. 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 Reopen, 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.

Field	Description
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.
External ID	Allows storing the Incident ID referrals from a different platform. **Note:** Click **Send to Archer** to generate the External ID. The ID generated is automatically stored as External ID.
Time to Acknowledge	Displays the time taken to assign an Incident after creating it.
Time to Detect	Displays the time taken for completing the task after the Incident is assigned.
Time to Resolve	Displays the time taken for closing the task after the Incident is created.
Persisted Status	Displays the persist status of the Incident. The status can be Complete, Partial, or None (-).
MITRE ATT&CK Tactics	Displays the tactic associated with the incident.
MITRE ATT&CK Techniques	Displays the technique associated with 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.

Option	Description
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.
More Actions drop-down	Allows you to perform a list of actions for the selected incident: • Create Report • Schedule Report • Retention Usage • Events Retention • Export

Incident Details View

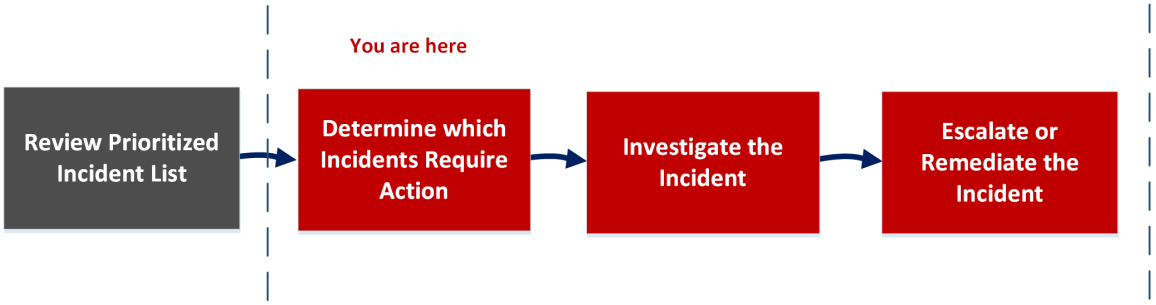
In the Incident Details view (Respond > Incidents > click an ID or NAME hyperlink in the Incidents List), you can view and access extensive incident details. The Incident Details view contains multiple panels that provide the following benefits:

- **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.
- **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.
- **History**: View all the actions performed by the user on any incident.
- **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.

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.



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 on the Nodal Graph
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 the Investigate > Events View
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 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

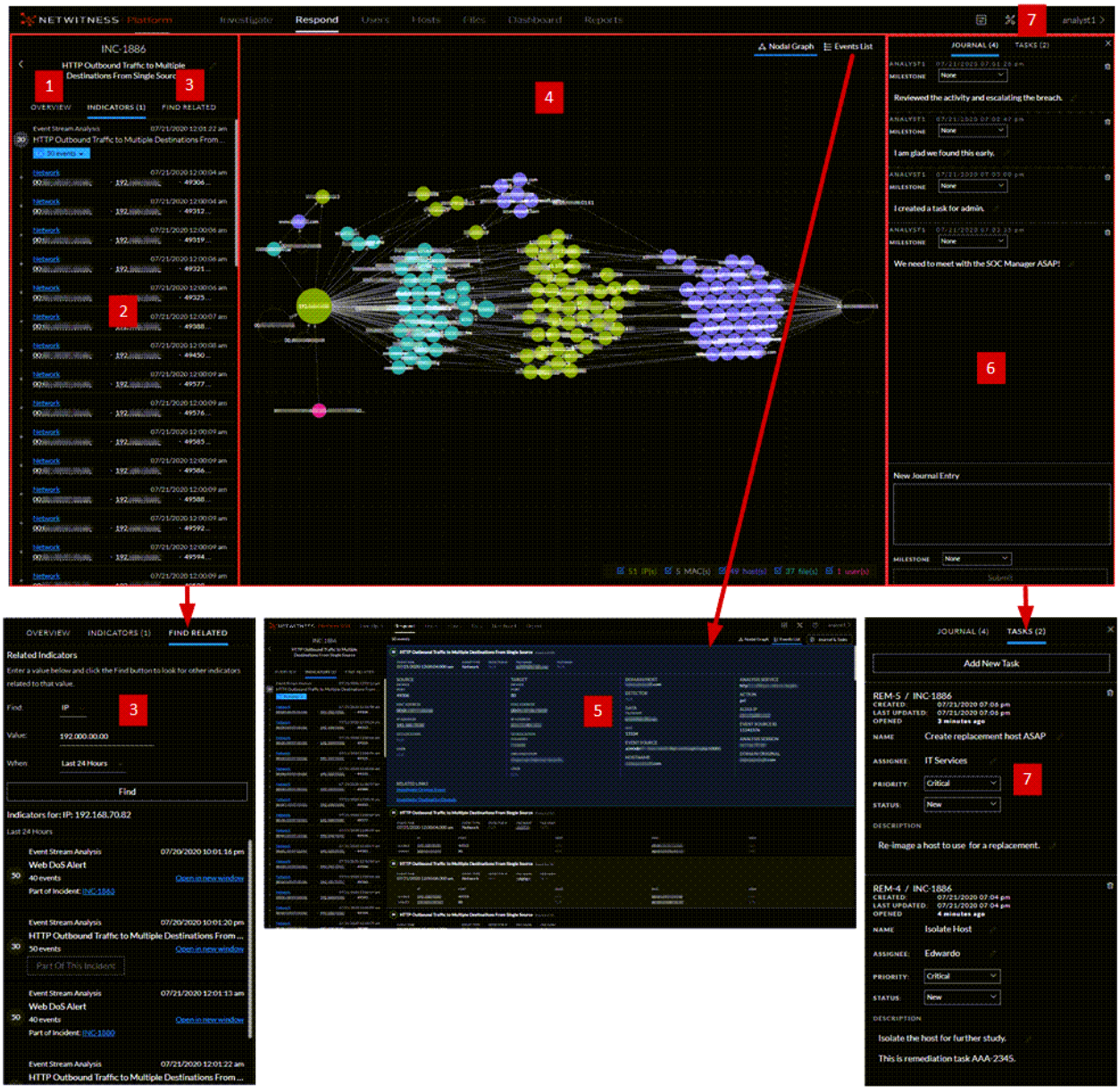
*You can complete these tasks here (that is, in the Incident Details view).

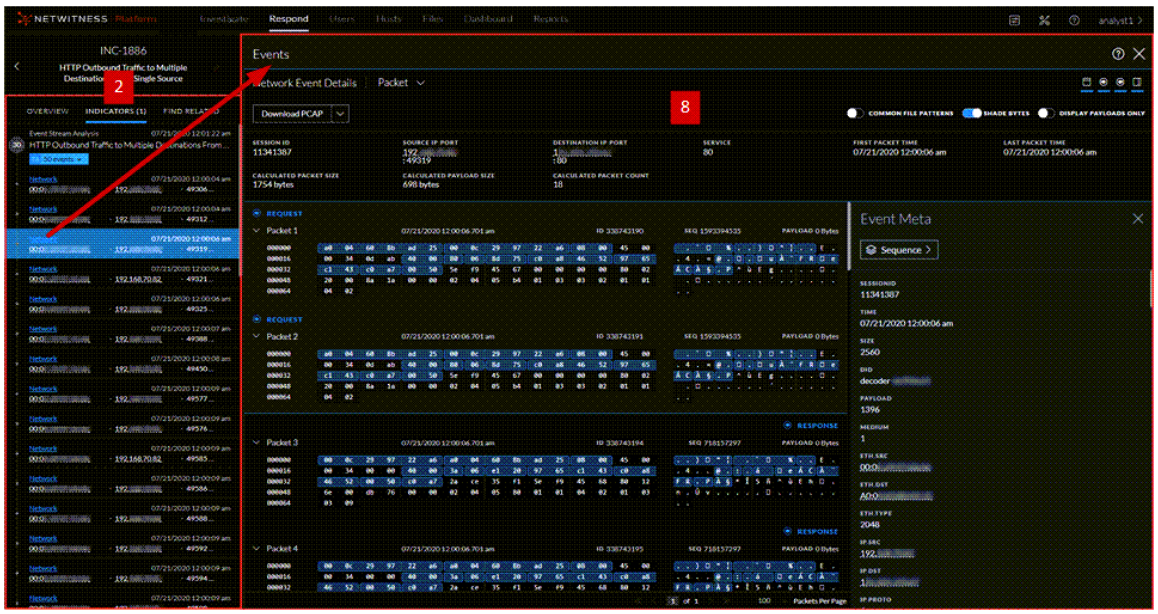
Related Topics

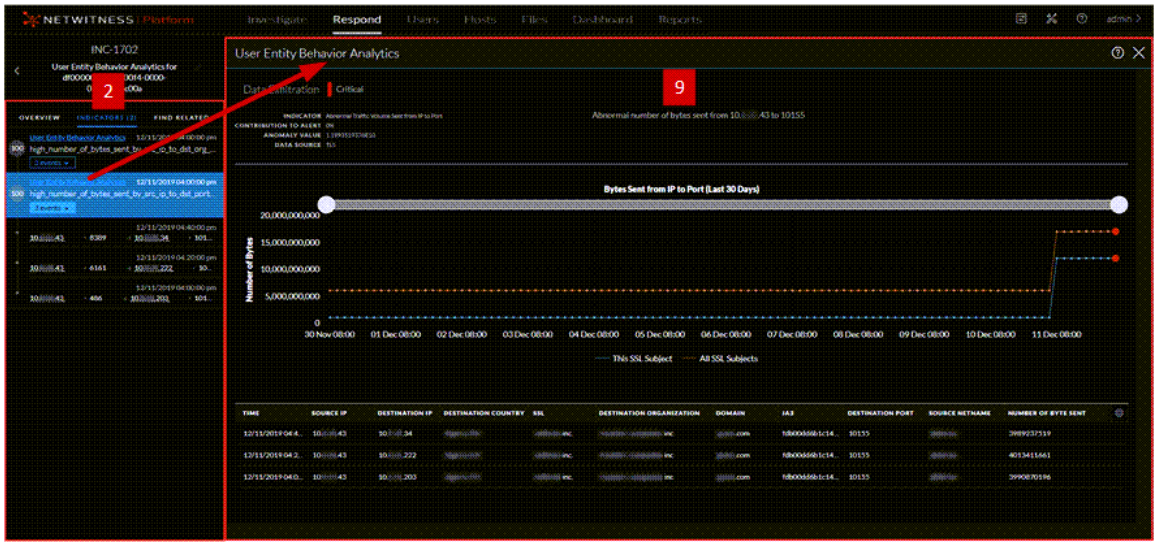
- Incidents List View
- Determine which Incidents Require Action
- Investigate the Incident
- Escalate or Remediate the Incident

Quick Look

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




NETWITNESS Platform
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
INC-1886
HTTP Outbound Traffic to Multiple Destinations from Single Source
2
Events
Network Event Details
Packet
8
Download PCAP
Event Meta
Sequence
Packet 1
Packet 2
Packet 3
Packet 4
REQUEST
RESPONSE


NETWITNESS Platform
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
INC-1702
User Entity Behavior Analytics
2
User Entity Behavior Analytics
9
Abnormal number of bytes sent from 10.[redacted].43 to 10155
Bytes Sent from IP to Port (Last 30 Days)
Number of Bytes
20,000,000,000
15,000,000,000
10,000,000,000
5,000,000,000
0
30 Nov 08:00
01 Dec 08:00
02 Dec 08:00
03 Dec 08:00
04 Dec 08:00
05 Dec 08:00
06 Dec 08:00
07 Dec 08:00
08 Dec 08:00
09 Dec 08:00
10 Dec 08:00
11 Dec 08:00
This SSL Subject
All SSL Subjects
TIME
SOURCE IP
DESTINATION IP
DESTINATION COUNTRY
SSL
DESTINATION ORGANIZATION
DOMAIN
IAJ
DESTINATION PORT
SOURCE NETNAME
NUMBER OF BYTE SENT

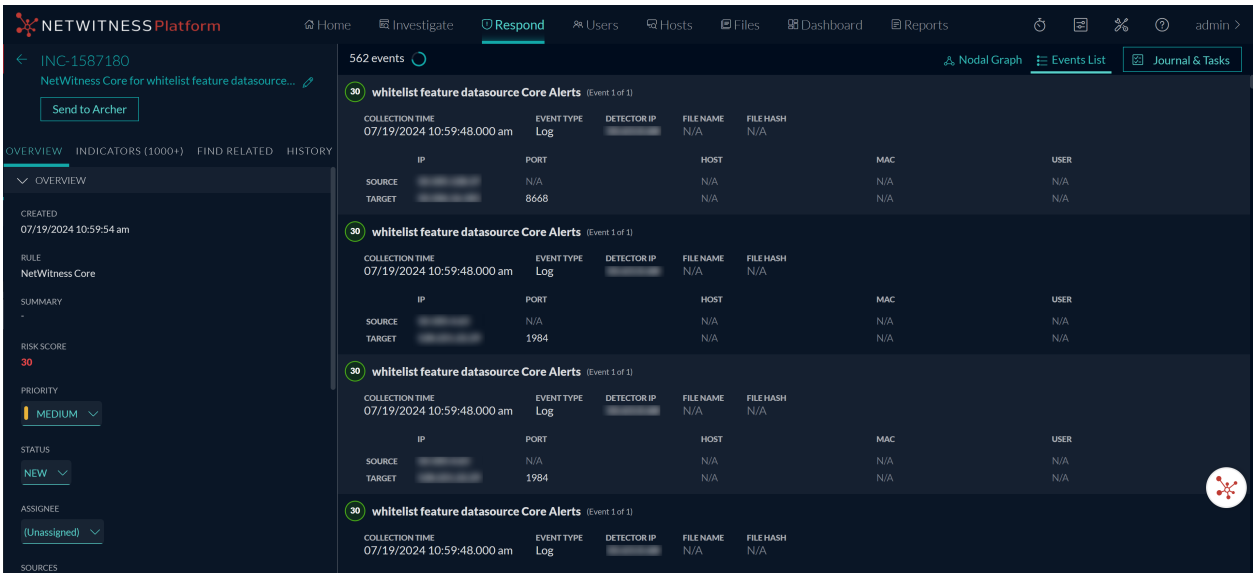
1. Overview (Click the Overview tab to view the Overview panel.)
2. Indicators Panel
3. Related Indicators Panel (Click the Find Related tab to view it.)
4. Nodal Graph
5. Events List (Click the top of an event in the Events List to view event details.)
6. Journal Panel
7. Tasks Panel (Click the Tasks tab to view it.)
8. Events (Click an event type hyperlink in the Indicators panel, such as Network, to view the Events view from Investigate for a specific indicator event.)
9. UEBA (Click a User Entity Behavior Analytics hyperlink in the Indicators panel to view UEBA.)
10. History Panel

Note: Your Incident Details view may not look like these diagrams because the layout changed in NetWitness 11.3.2 and later versions.
The Related tab is renamed as the Find Related tab and is located on the left-side panel.
The journal is open by default on the right-side panel. When the journal is closed, the Journal & Tasks button enables easy access to notes and tasks.

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 Incident Overview Panel topic provides details.

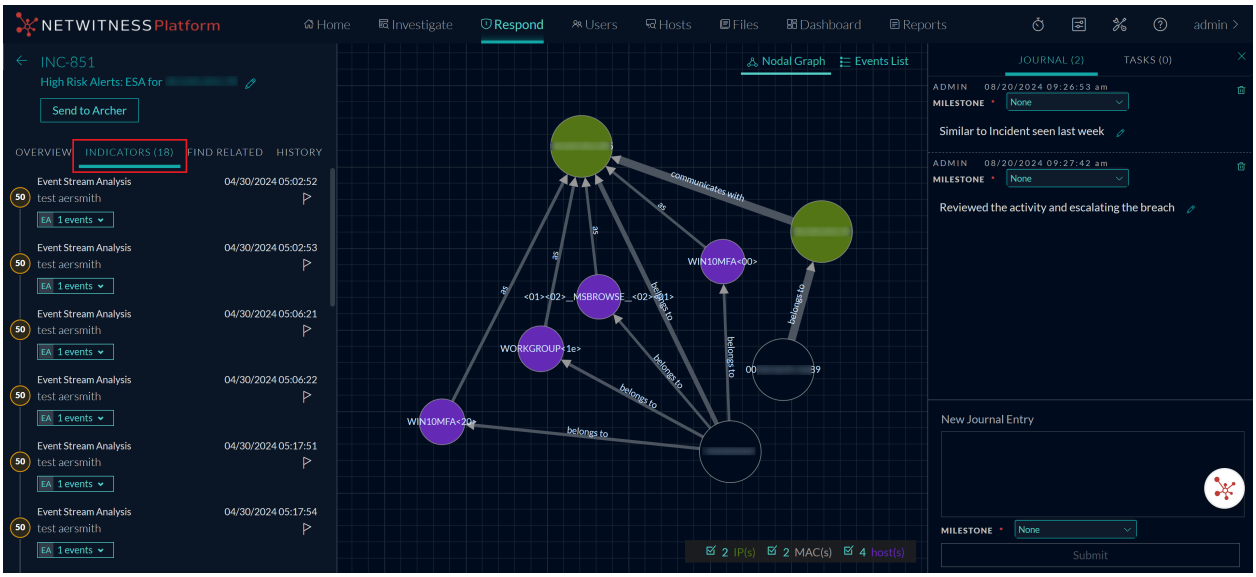
To view the Overview panel in the Incident Details view, click the **Overview** tab in the left panel.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
INC-1587180
NetWitness Core for whitelist feature datasource...
Send to Archer
OVERVIEW
INDICATORS (1000+)
FIND RELATED
HISTORY
OVERVIEW
CREATED
07/19/2024 10:59:54 am
RULE
NetWitness Core
SUMMARY
RISK SCORE
30
PRIORITY
MEDIUM
STATUS
NEW
ASSIGNEE
(Unassigned)
SOURCES
562 events
Nodal Graph
Events List
Journal & Tasks
30 whitelist feature datasource Core Alerts (Event 1 of 1)
COLLECTION TIME
07/19/2024 10:59:48.000 am
EVENT TYPE
Log
DETECTOR IP
FILE NAME
N/A
FILE HASH
N/A
IP
PORT
HOST
MAC
USER
SOURCE
TARGET
8668
1984

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, click the **Indicators** tab.



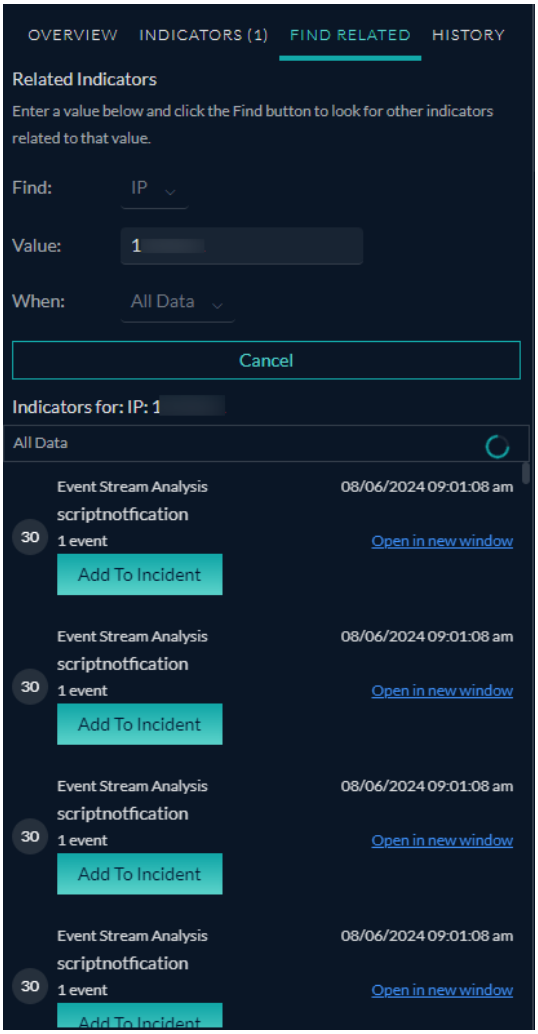
Data source information is shown below the names of the indicators. You can also see the creation date and time of the indicator and the number of events in the indicator. In the Indicators panel, you can drill deeper into the events associated with the listed indicators to get a better understanding of the events.

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

Related Indicators Panel

The Related Indicators panel enables you to search the NetWitness 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.

To view the Related Indicators panel, in the left panel of the Incident Details view, click the **Find Related** tab.



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

Field	Description
Find	Select the entity that you would like to locate in the alerts. For example, IP.
Value	Type the value of the entity. For example, type the actual IP address of the entity.
When	Select a time range to search for the alerts. For example, Last 24 hours.

Field	Description
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.

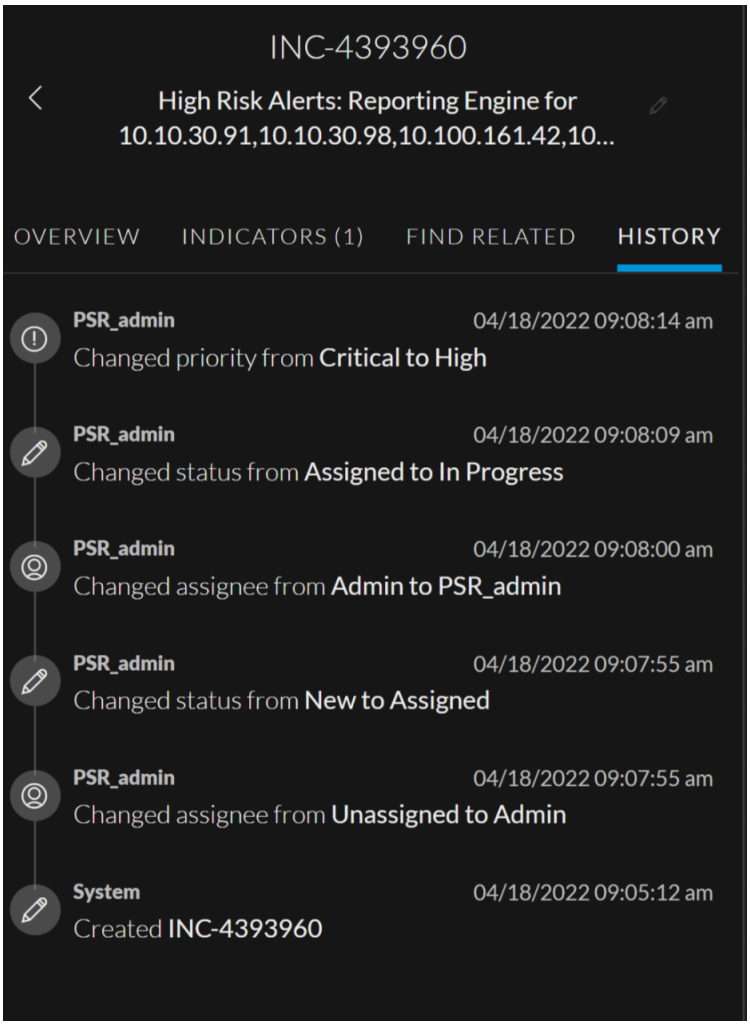
Option	Description
Indicators For:	Shows the search results.
Open in new window link	Shows alert details for the indicator.
Add To Incident button	Adds the related indicator to the incident. The related indicator adds to the Indicators panel.
Part Of This Incident button	Shows that the indicator is already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

History Panel

The History panel displays every action performed by the user on an incident. The various actions performed on an incident are as shown below

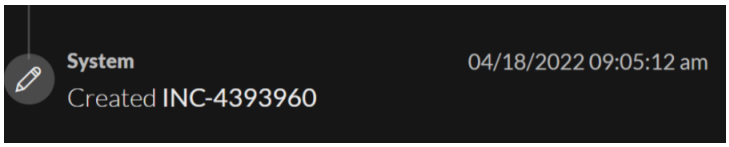
- Incident Assignee Change
- Incident Status Change
- Incident Priority Change
- Incident Creation

Every time a user performs an action on an incident, the date and time also gets recorded and is displayed in the panel. Consider the following example

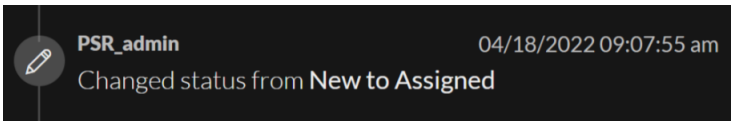


The different actions performed by the user are described below

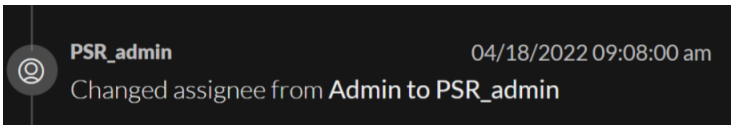
- In this example, the Incident INC-4393960 was created by the user (System) on 18/04/2022 at 09:05:12 am.



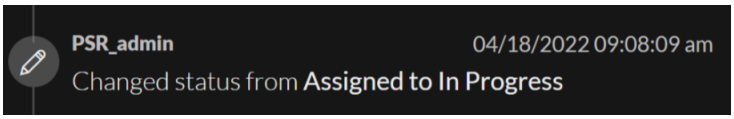
- After the incident creation, PSR_admin assigned the incident to Admin on 18/04/2022 at 09:07:55 am. Hence, the status of the incident is changed from New to Assigned.



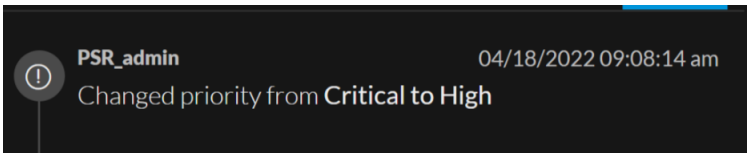
- Later, PSR_admin changed the Incident assignee from Admin to PSR_admin on 18/04/2022 at 09:08:00 am.



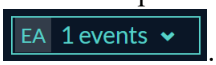
- After changing the assignee, PSR_admin changed the Incident status from Assigned to In Progress on 18/04/2022 at 09:08:09 am.



- Later, the Incident priority was changed from Critical to High on 18/04/2022 at 09:08:14 am by PSR_admin.

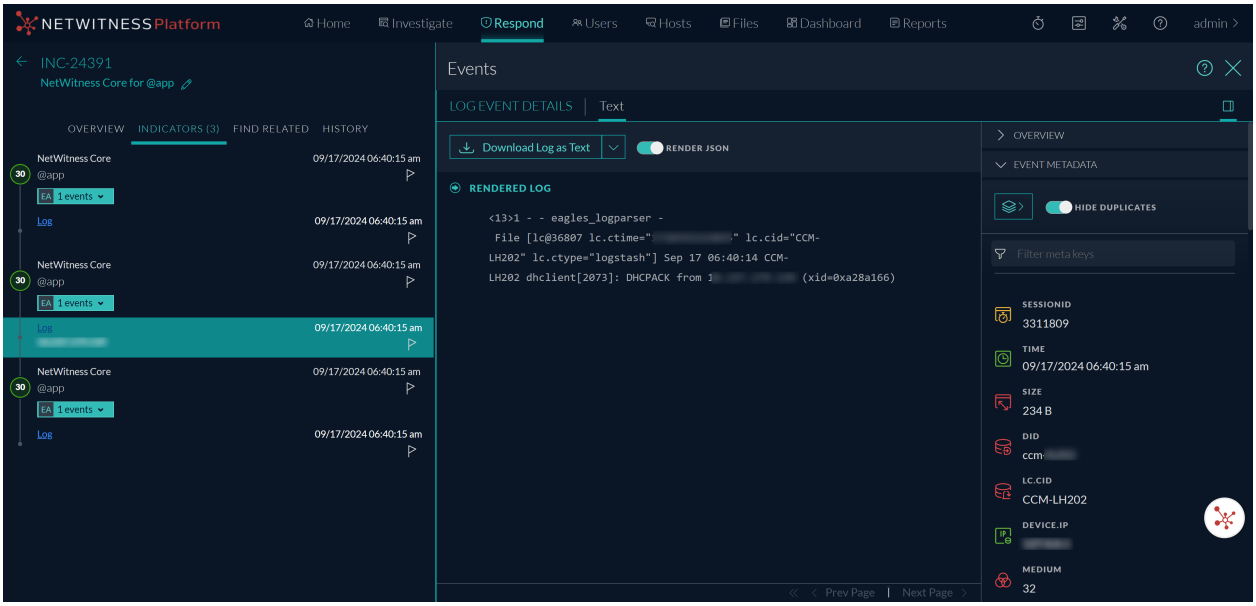


Events

You can perform an event analysis from the Indicators panel. Event counts preceded by an **EA** (event analysis) icon have event reconnaissance information available: 

. You can select an event type hyperlink, such as Network, to access the Events panel for the selected event.

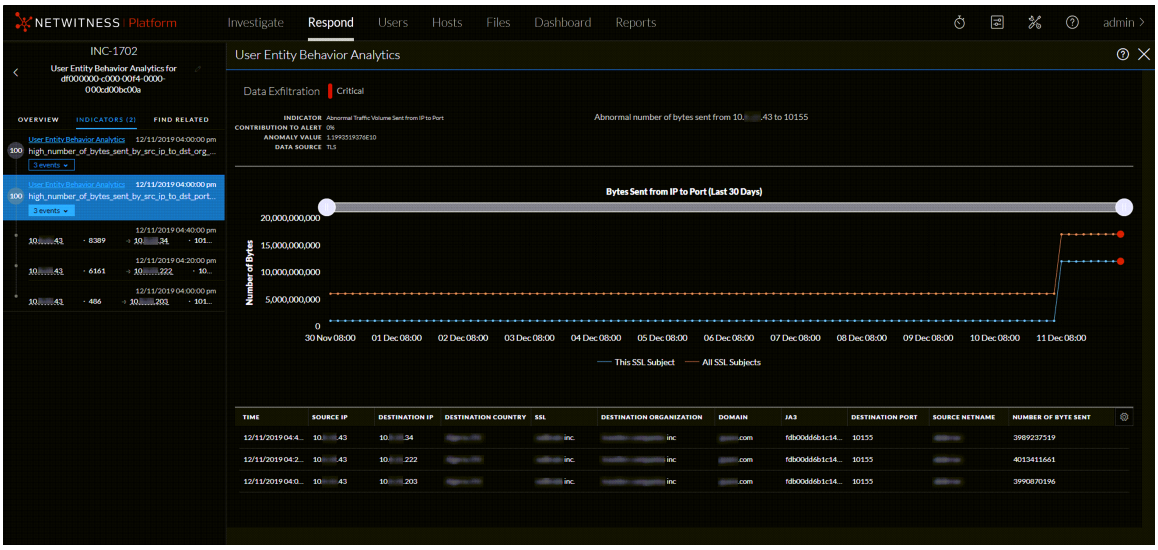
In the Events panel, you can view raw events and metadata with interactive features that enhance your ability to find meaningful patterns in the data. You can examine network, log, and endpoint events. The Events panel in the Respond view shows the Events view from Investigate for specific indicator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



Note: Migrated incidents from NetWitness versions before 11.2 will not show the Events 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 11.5, you will also not be able to view the Events panel in the Respond view for those incidents.

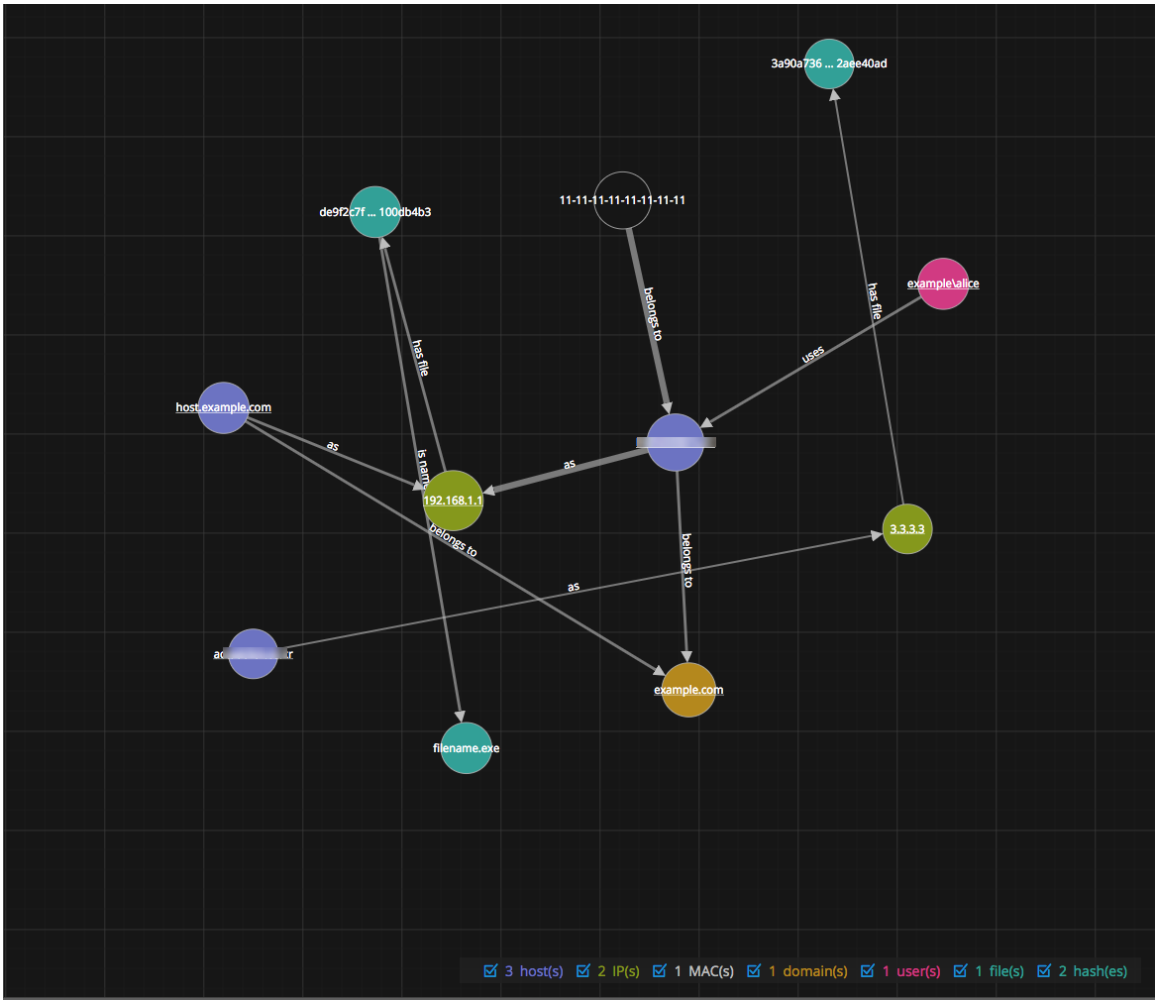
User Entity Behavior Analytics

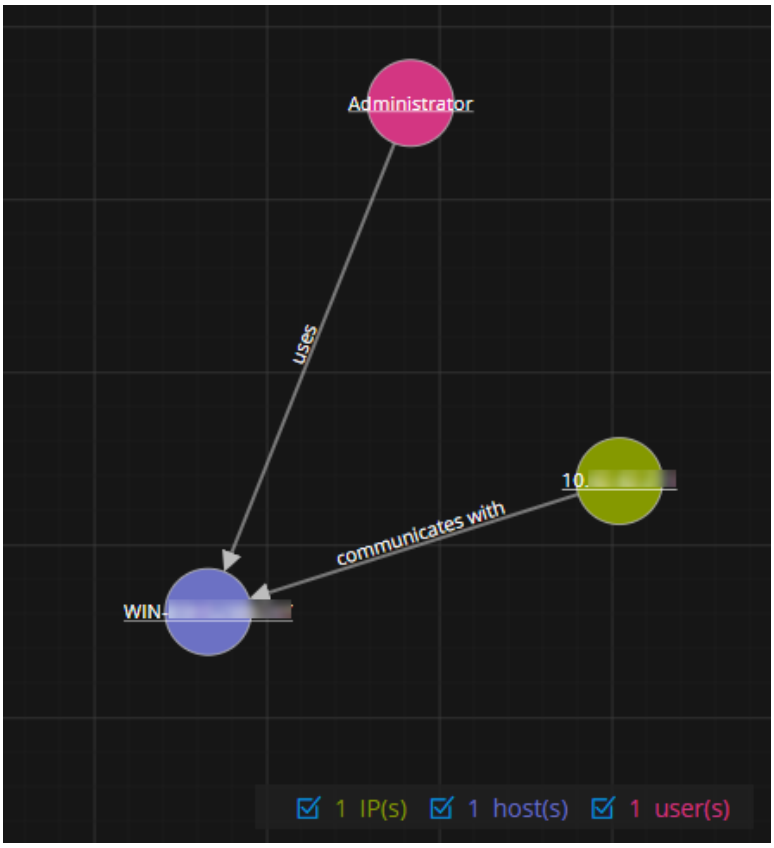
NetWitness UEBA (User and Entity Behavior Analytics) is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all users and entities in your network environment. You can access UEBA from the Respond Incident Details view Indicators panel. Indicators with 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 represented by an IP address, MAC address, user, host, domain, file name, or file hash.





Nodes

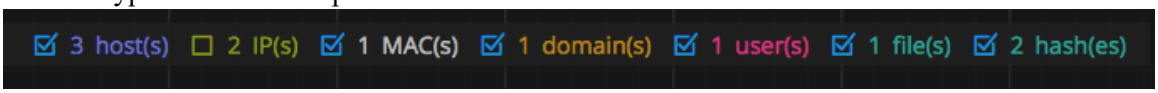
In the nodal graph, circles represent nodes. The following table describes the nodal graph node types.

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	If a host is associated with a domain, you can see a domain node.
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 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.

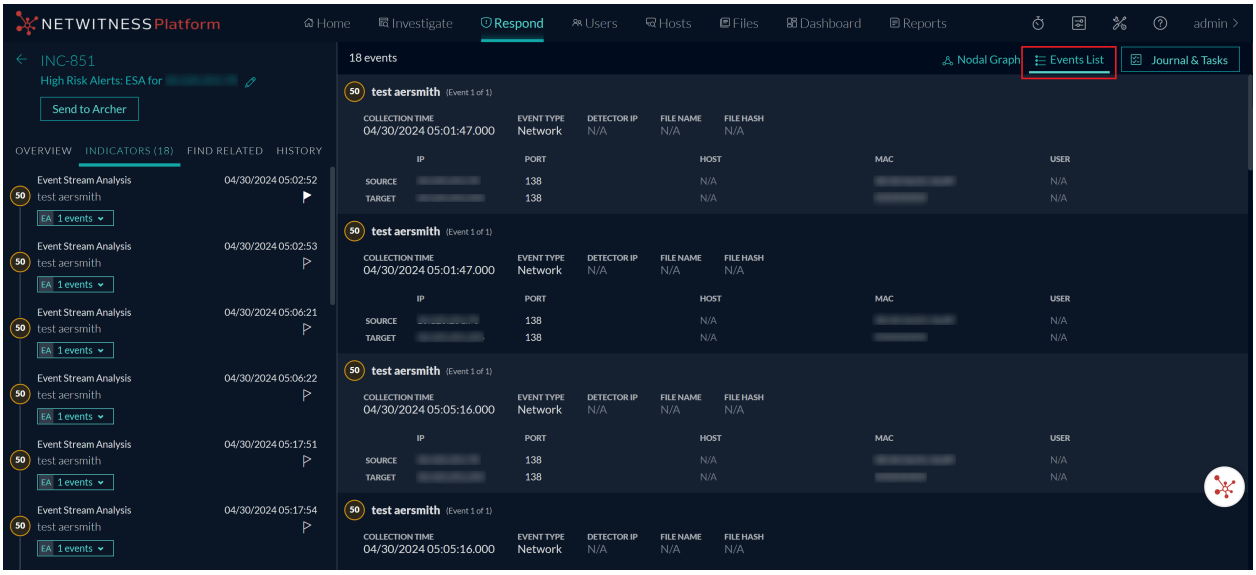
Arrow	Description
Communicates with	An arrow between a Source machine node (IP address or MAC address) and a Destination machine node labeled with "communicates with" shows the direction of the communication.
Has file	An Arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has file " 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.
Calls	(This arrow is available in NetWitness Platform 11.4 and later.) An arrow between two file hash (checksum) nodes labeled with "calls" indicates the direction of the interaction between the associated files. The source file hash "calls" the target (destination) file hash, which indicates that the source file associated with the source file hash is performing an action on the target file associated with the target file hash.
As	(This relationship type represents attributes of the connected node.) 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.
Is named	(This relationship type represents attributes of the connected node.) 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	(This relationship type represents attributes of the connected node.) 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.

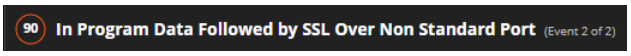
The following figure shows an Events List for network events.



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**.

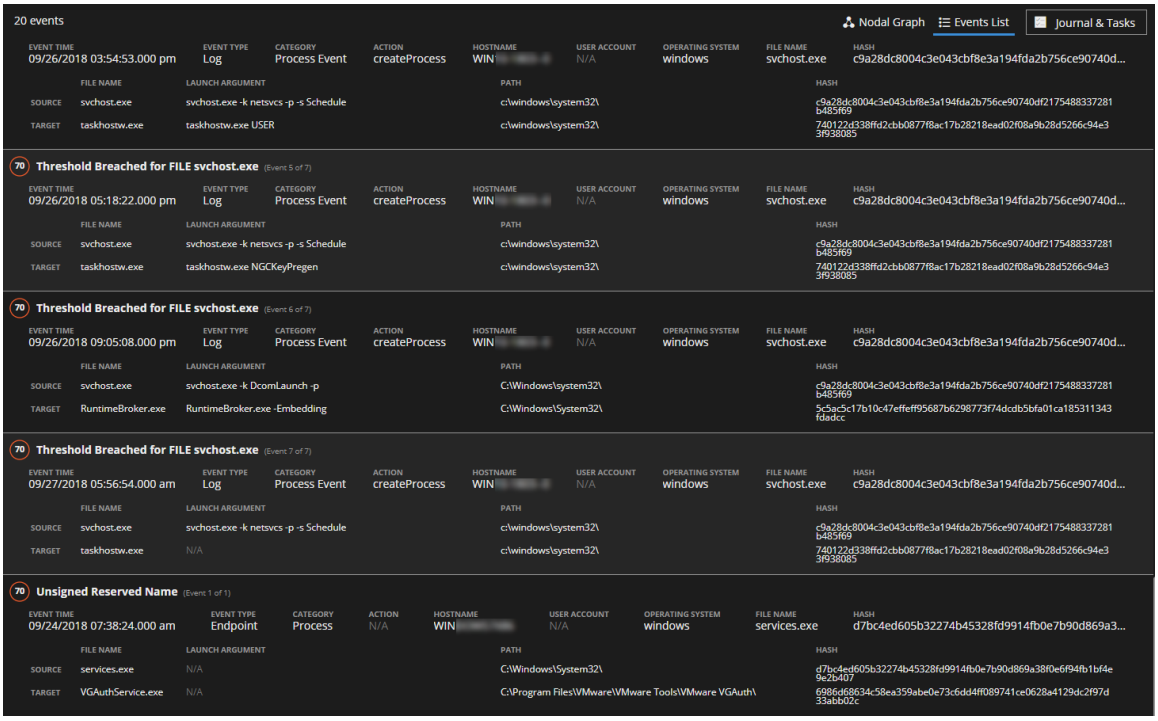


The following table describes the fields in the Events List for network or log events.

Field	Description
COLLECTION 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.

Field	Description
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.



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.

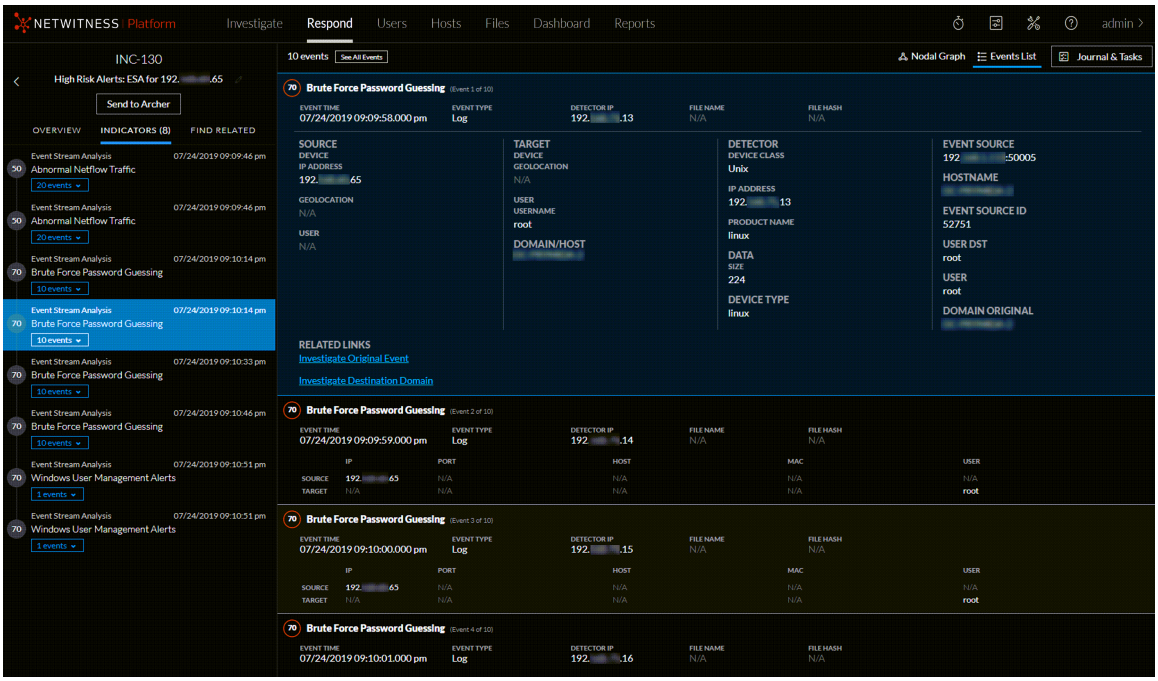
Field	Description
EVENT TIME	Shows the time the event occurred.
EVENT TYPE	Shows the type of alert, such as Endpoint or Log. NetWitness Endpoint events have an `Endpoint` event type. NetWitness Endpoint events from version 4.4.x and earlier can have an Event Type that shows the origin of the event.
CATEGORY	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 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 `nwendpoint` for NetWitness Endpoint.

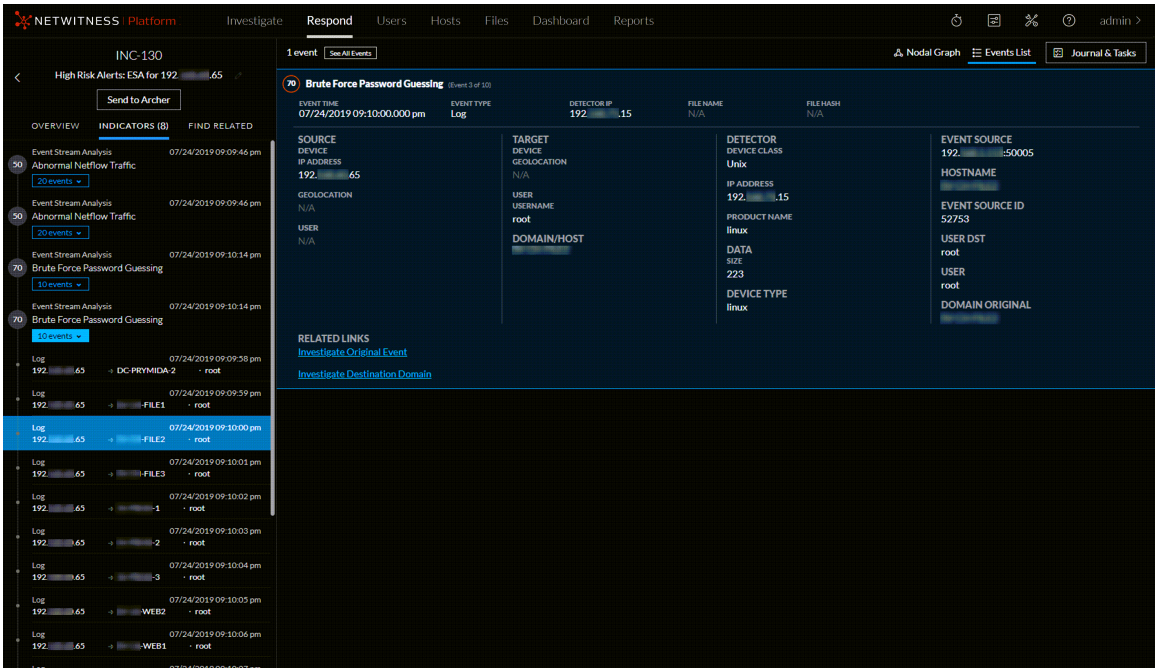
Event Details

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.

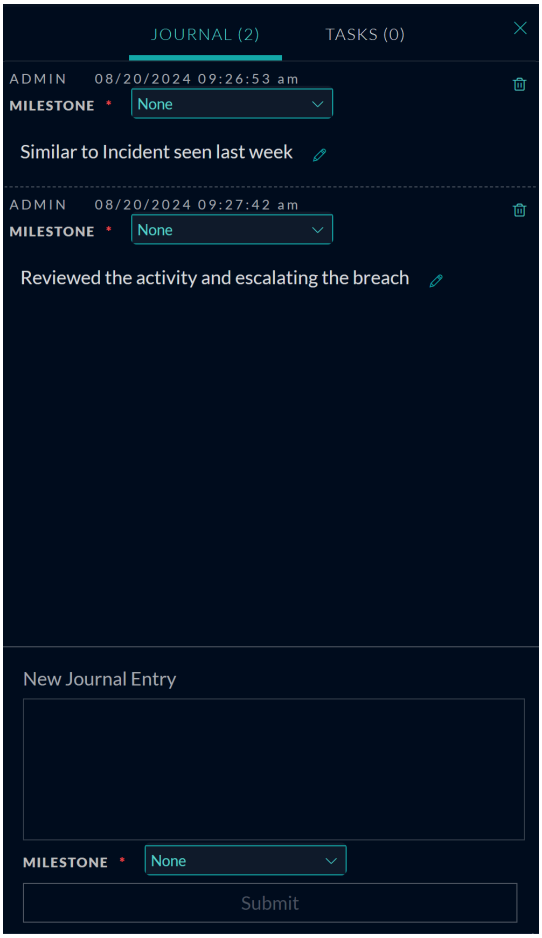


The following figure shows a specific indicator event selected in the Indicators panel. Information about the selected event appears in the Events List on the right.



Journal Panel

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

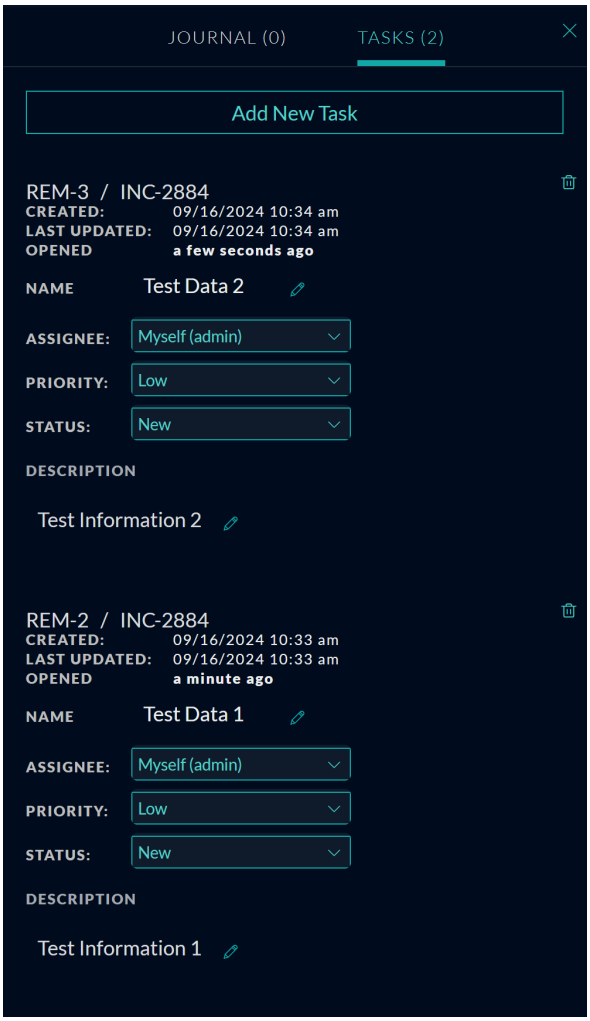


The following table describes the New Journal Entry options.

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

Tasks Panel

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

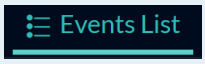


The following table describes the Task fields.

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

Field	Description
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.

Toolbar Actions

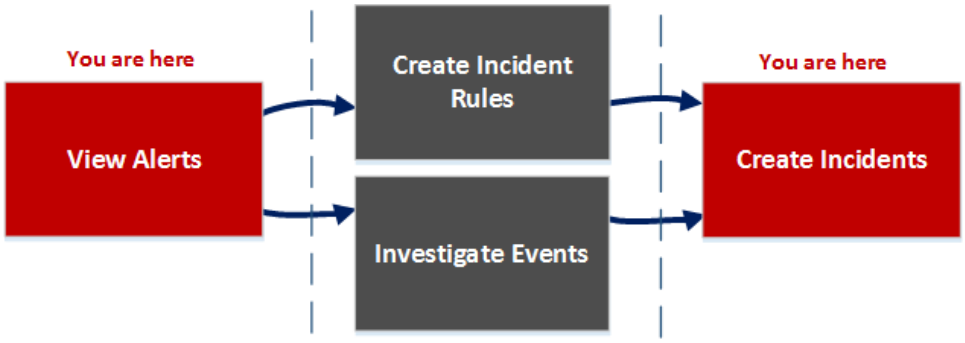
Option	Description
	(Back to Incidents) Enables you to navigate back to the Incidents List view.
	Closes the panel.
	Deletes the entry, such as a journal entry or task.
Priority button	(In the Overview panel) Allows you to change the Priority of one or more selected incidents in the Incidents List.
Status button	(In the Overview panel) Allows you to change the Status of one or more selected incidents.
Assignee button	(In the Overview panel) Allows you to change the Assignee of one or more selected incidents.
	Enables you to view the Nodal Graph.
	Enables you to view the incident Events List. Clicking the top of an event enables you to view the event details below it.
	Enables you to view incident notes and tasks.
 (Journal, Tasks, and Related)	(This option is available in NetWitness Version 11.3.1 and earlier 11.x versions.) Enables you to view the Journal, Tasks, and Related Indicators panels.
	Enables you to show or hide the event header, request, response, and metadata in the Events panel in the Respond Incident Details view. For more information about event analysis, see "Events View" in the *NetWitness Investigate User Guide*.

Alerts List View

The Alerts List view (Respond > Alerts) enables you to view all of the threat alerts and indicators received by NetWitness in one location. This can include alerts received from ESA Correlation Rules, 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. 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 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.*	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 NetWitness 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 *NetWitness Respond Configuration Guide*.
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

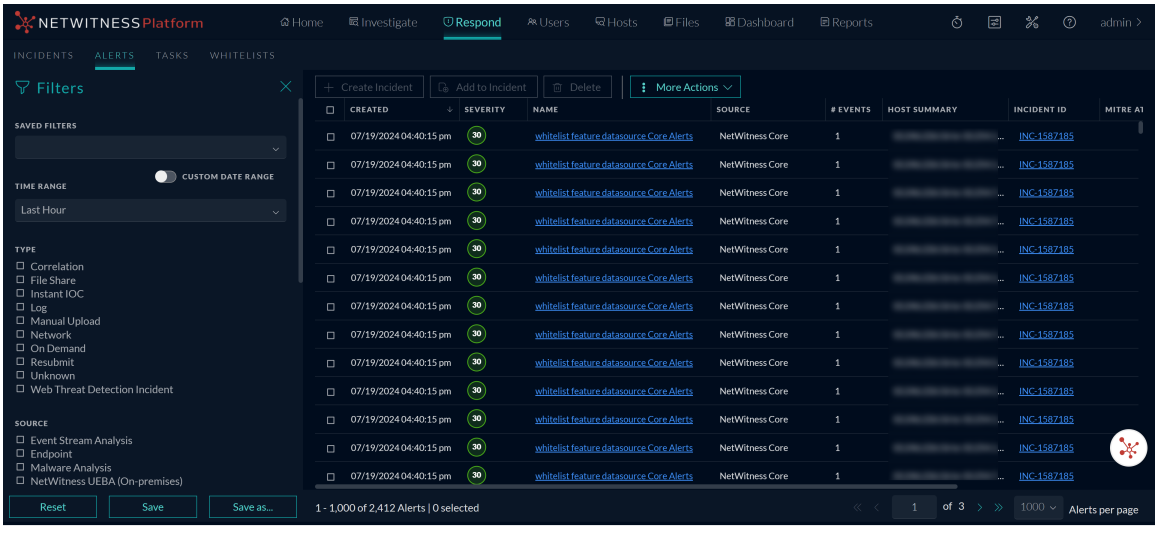
*You can complete these tasks here (that is, in the Alerts List view).

Related Topics

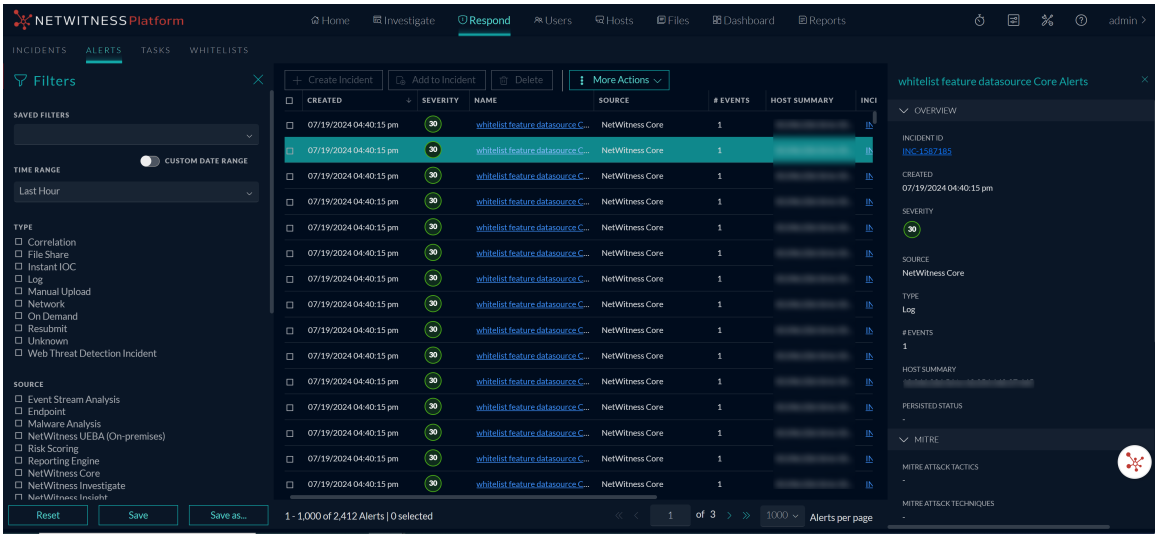
- Alert Details View
- Reviewing Alerts

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. The following figure shows the Filters panel on the left.

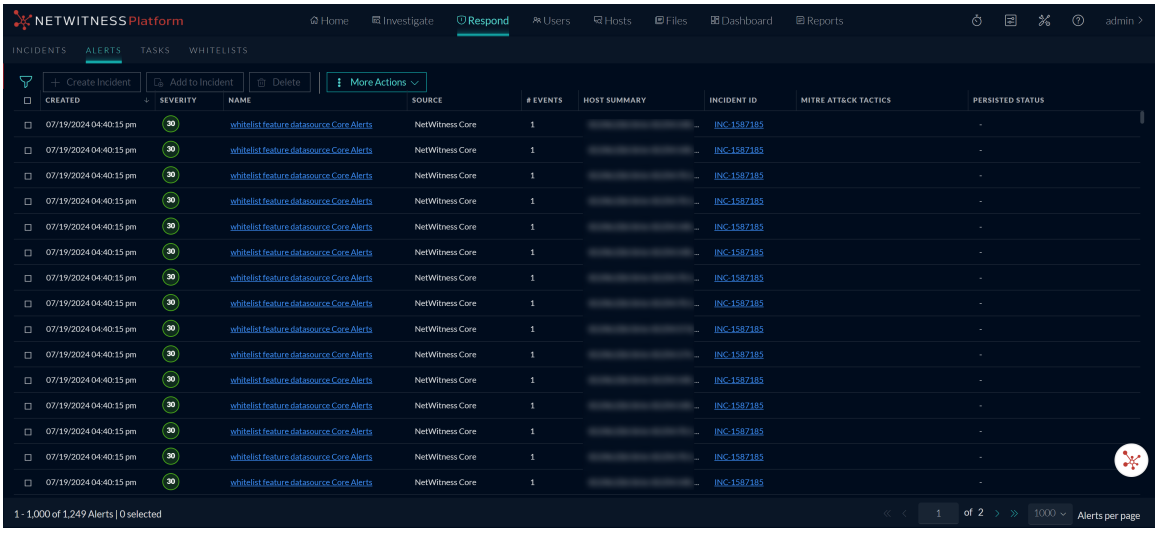


The Alerts List view consists of a Filters panel, an Alerts List, and an Alert Overview panel. You can click an alert in the Alerts list to view the Alert Overview panel on the right.

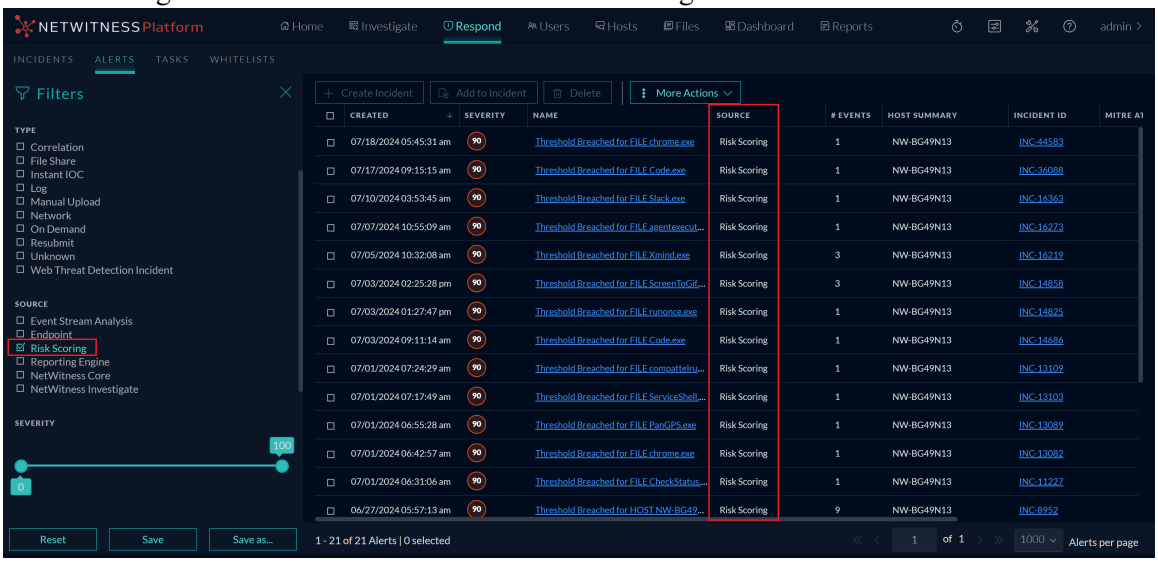


Alerts List View

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



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



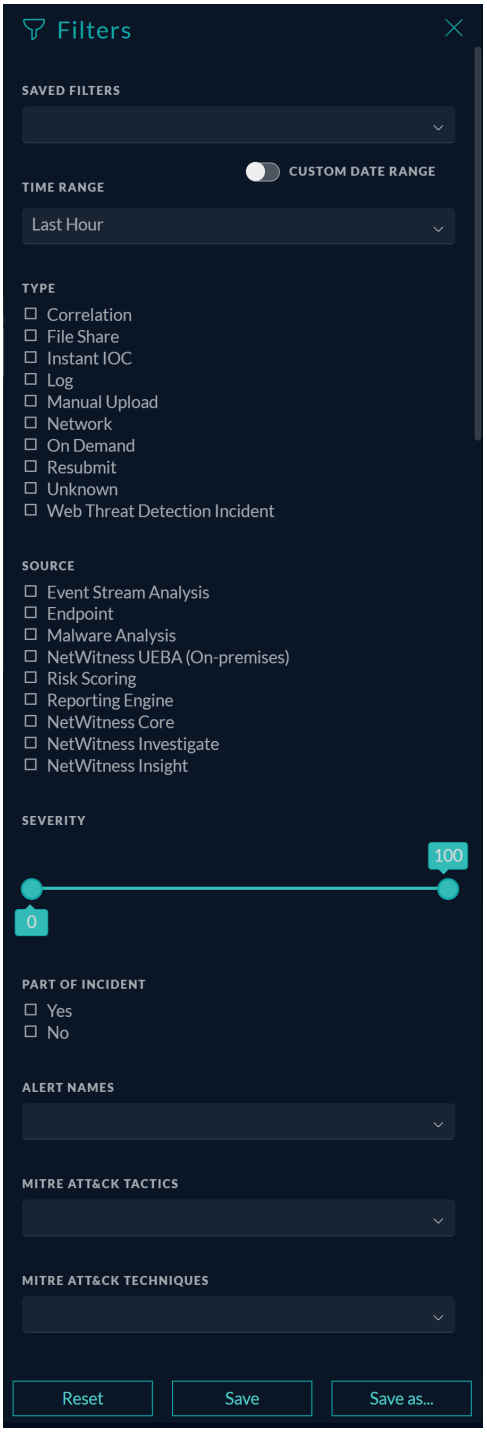
The following table describes the columns in the Alerts List.

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	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, ESA correlation rules, Reporting Engine, Risk Scoring, and many others. **Note:** - From 12.3.1 and later, the alert source filter panel displays only the sources installed in your instance of NetWitness and won't display all possible sources. If a user deletes a host / service on their NetWitness Instance, any source associated with that host / service will be marked as decommissioned. For Ex. ESA Primary is deleted in the hosts page, the ESA source will be marked as decommissioned, the source decommissioned message (**source has been decommissioned**) is displayed in the alert source filter panel.
# 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.
MITRE ATT&CK Tactics	Shows the particular Tactic associated with each alert.
Persisted Status	Shows the persist status of the Alert. The status can be Complete, Partial, or None (-).

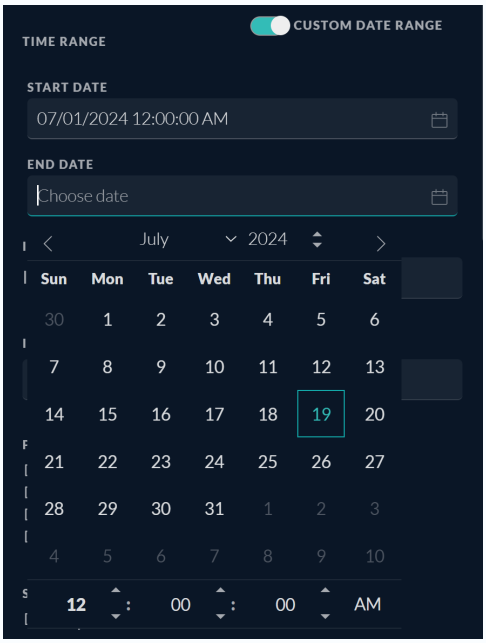
At the bottom of the list, you can see the number of alerts on the current page, the total number of alerts, and the number of alerts selected. For example: **Showing 4 out of 4 items | 1 selected**

Alert 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.

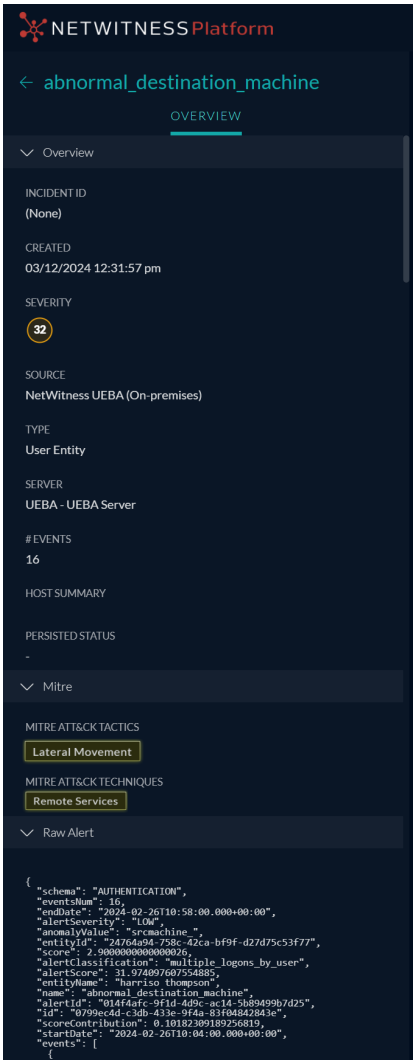
Option	Description
Saved Filters	You can select a saved filter to filter the alerts list. Saved filters are global. You can save a filter for other analysts to use and you can use any saved filter. Saved filters are also available for use on the Springboard landing page. Filters used in the Springboard cannot be deleted. (This option is available in NetWitness Platform 11.5 and later.)
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.
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	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
Source	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), 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 device_type of `nwendpoint`, the source changes to Endpoint.

Option	Description
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 names of the alerts being filtered. You can use this filter to search for all alerts generated by a specific rule, for example, Direct Login to an Administrative Account.
MITRE ATT&CK Tactics	Allows you to select the tactic associated with the alert.
MITRE ATT&CK Techniques	Allows you to select the technique associated with the alert.
Reset	Removes your filter selections. If you reset filters on a saved filter, it takes you to the default empty filter.
Save	Saves the currently applied alerts filter or updates a saved filter. For a new filter, choose a unique name that contains 1-256 alphanumeric characters, underscores, or hyphens. (This option is available in NetWitness Platform 11.5 and later.)
Save As	Saves the currently applied alerts filter for future use. Choose a unique name that contains 1-256 alphanumeric characters, underscores, or hyphens. (This option is available in NetWitness Platform 11.5 and later.)

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**

Alert 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.

Field	Description
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.
Source	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, NetWitness UEBA (On-premises), NetWitness Insight, NetWitness UEBA (Cloud), Malware Analysis, ESA correlation rules, Reporting Engine, 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 device_type of `nwendpoint`, the source changes to Endpoint.
Type	Indicates the type of events in the alert, for example, logs, network sessions, and so on. There can be multiple types listed. **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 `nwendpoint`, the source changes to Endpoint.
Server	Displays details of the UEBA Server from where the alert was triggered. For example, UEBA - UEBA Server. **Note:** This option is only available for UEBA servers, which can be UEBA servers 1 or 2.
# 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.
MITRE ATT&CK Tactics	Displays the tactic associated with the alert.
MITRE ATT&CK Techniques	Displays the technique associated with the alert.
Raw Alert	Shows the raw alert metadata.

Toolbar Actions

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

Option	Description

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 thePart of Incident section, select No.
Add to Incident button	(This option is available in NetWitness 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.
More Actions drop-down	Allows you to perform a list of actions for the selected incident: • Create Report • Schedule Report • Whitelist Alert • Export

Alert Details View

In the Alert Details view (Respond > Alerts > click on a row in the Alerts List), you can view the overview of an alert, such as the source of the alert, the number of events within the alert, Incident ID, if it is part of an incident. You can also view the raw alert that contains detailed information about the events.

Workflow

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

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

Note: You can also use NetWitness 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.	View Alerts
SOC Managers, Administrators	Create incident rules.	See "Create an Incident Rule for Alerts" in the *NetWitness Respond Configuration Guide*.
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

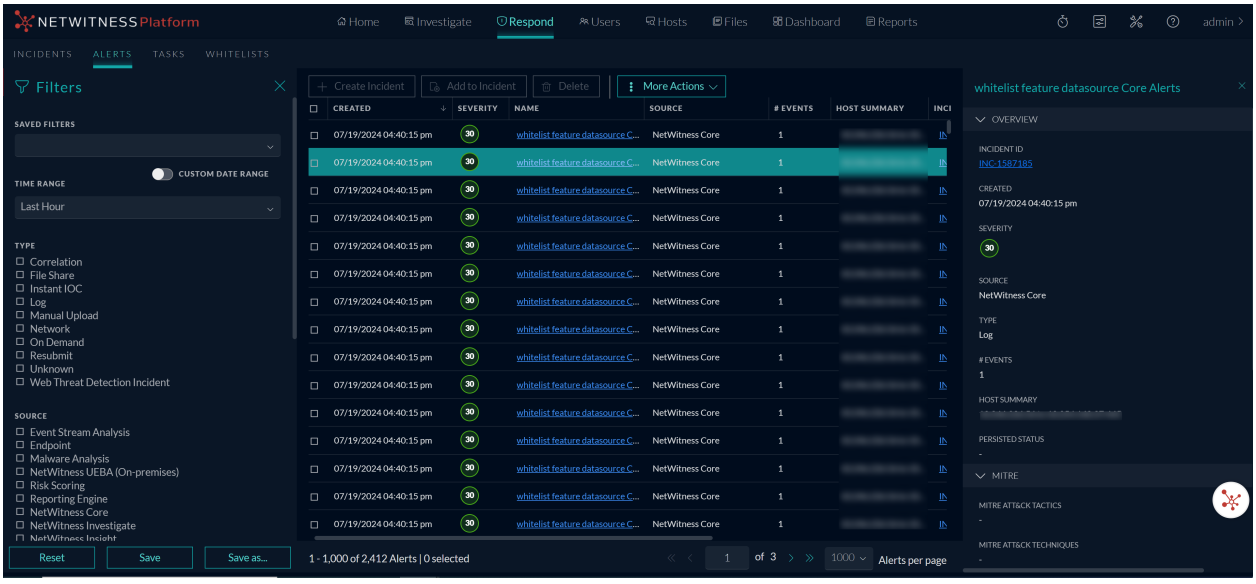
*You can complete these tasks here (that is, in the Alerts Details view).

Related Topics

- Alerts List View
- Reviewing Alerts

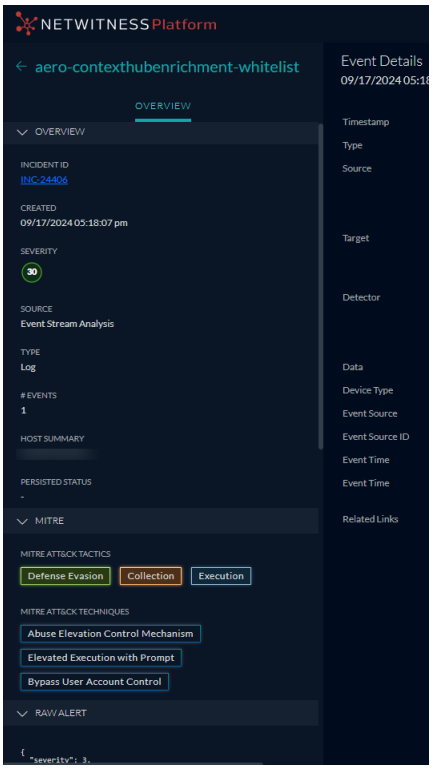
Quick Look

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



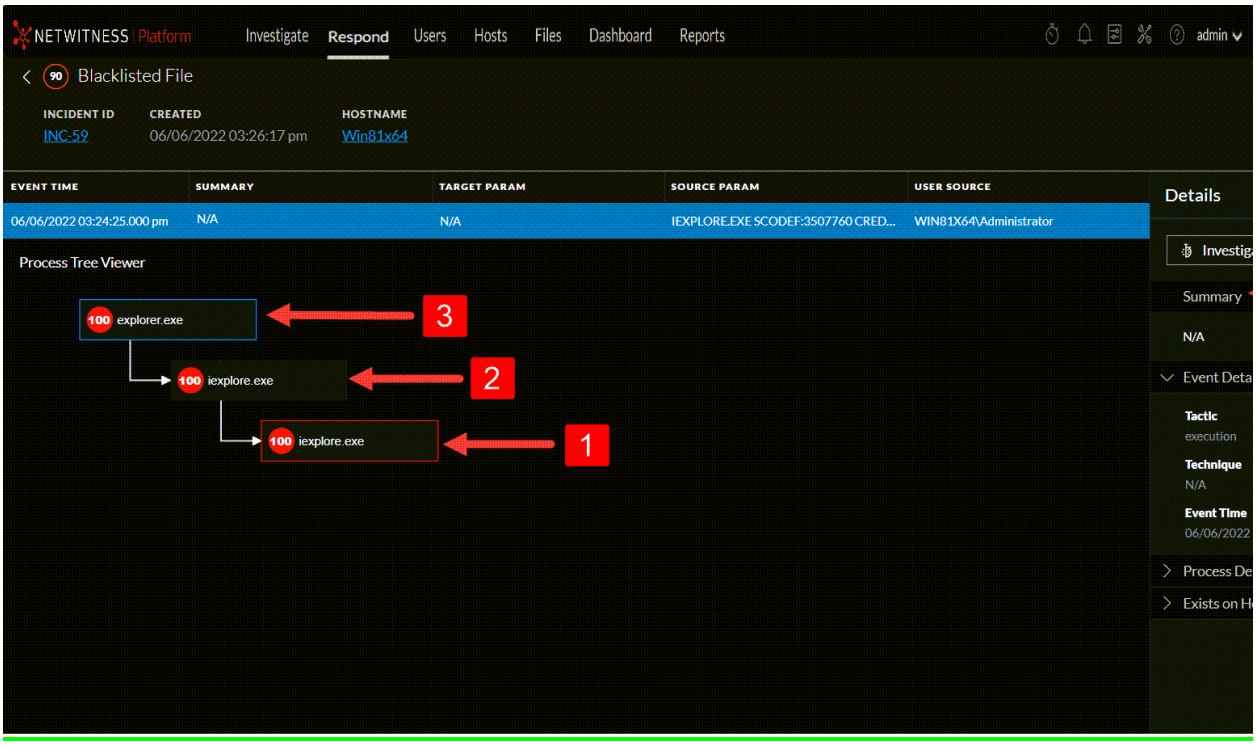
Overview Panel

The Overview panel shows basic summary information about a selected alert. The Overview panel on the Alerts List view contains the same information. The Alerts List view Alert Overview Panel topic provides details.



Events - Process Tree View

Click on an event name link to view the event details. The Process Tree Viewer opens and displays the process that caused the alerts and the processes it originated from.



1 -The process that caused the alert is highlighted with a red-colored outline.

2 & 3 - The processes from which the highlighted process originated.

4 - Summary of the alert.

5 - Event Details section shows the tactics, techniques, and event time stamp.

6 - Process Details section provides detailed insights about the selected process.

7 - Shows the details of Network Connections established by the process; You can view the network connections that took place up to ten minutes before and after the alert triggered time. Network connections details are available only for the process that caused the alert.

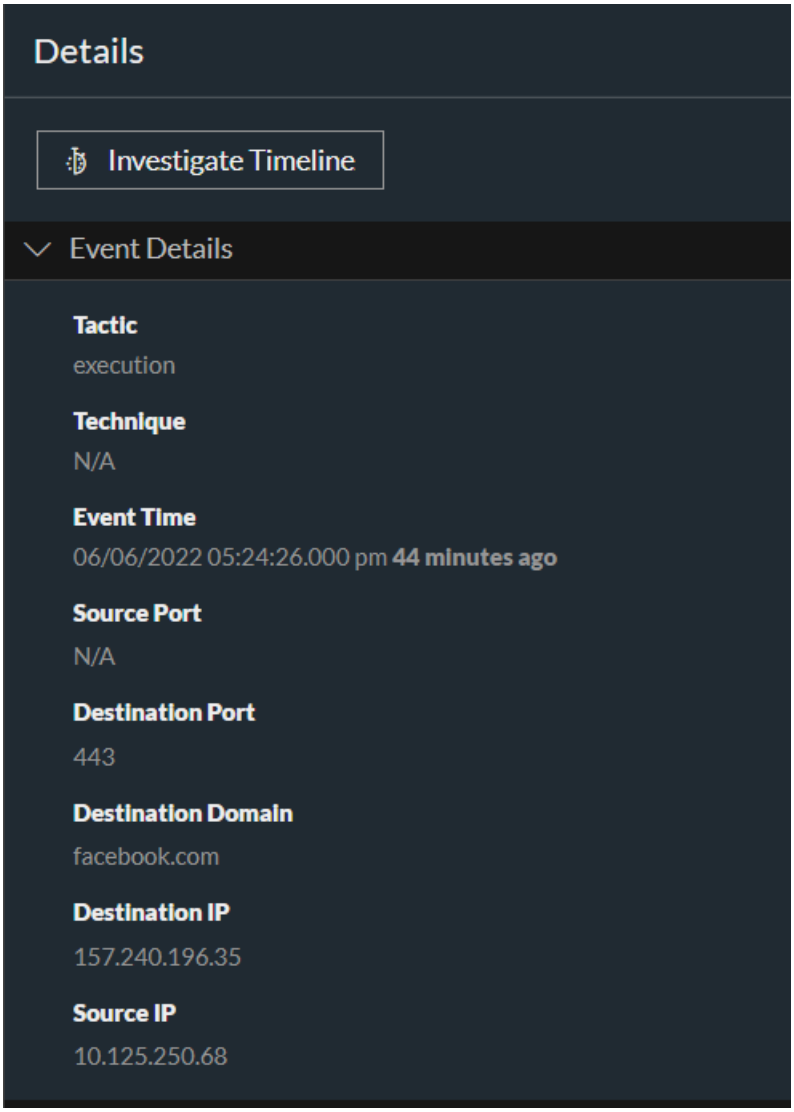
8 - Shows the name and a link to the host where the process exists.

Events List

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

Event Details

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



Event Details

The following table lists some event details section and subsections shown in the Event Details. This is not an extensive list.

Section	Subsection	Description
Summary		Shows a summary of the event.

Section	Subsection	Description
Event		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 destinationSee 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.

Name	Description
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 attibutes: 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.

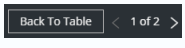
Event Source or Destination User Attributes

The following table lists attributes for an 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?

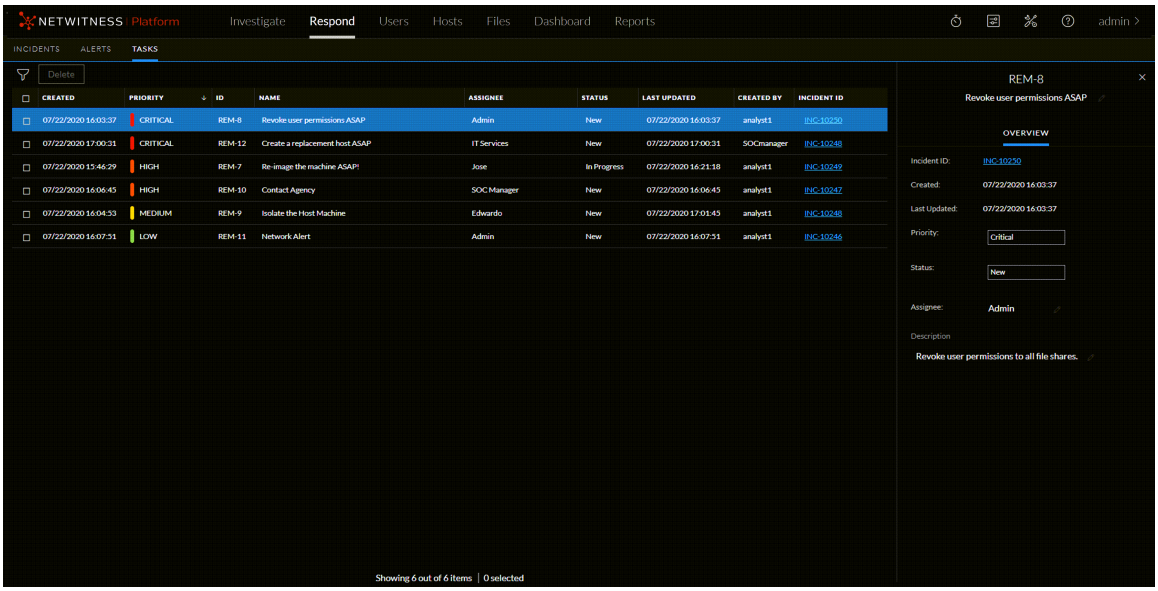
Role	I want to ...	Show me how
Incident Responders, Analysts	View tasks	View All Incident Tasks and View the Tasks Associated with an Incident
Incident Responders, Analysts	Filter tasks.	Filter the Tasks List
Incident Responders, Analysts	Create a task.	Create a Task
Incident Responders, Analysts	Find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

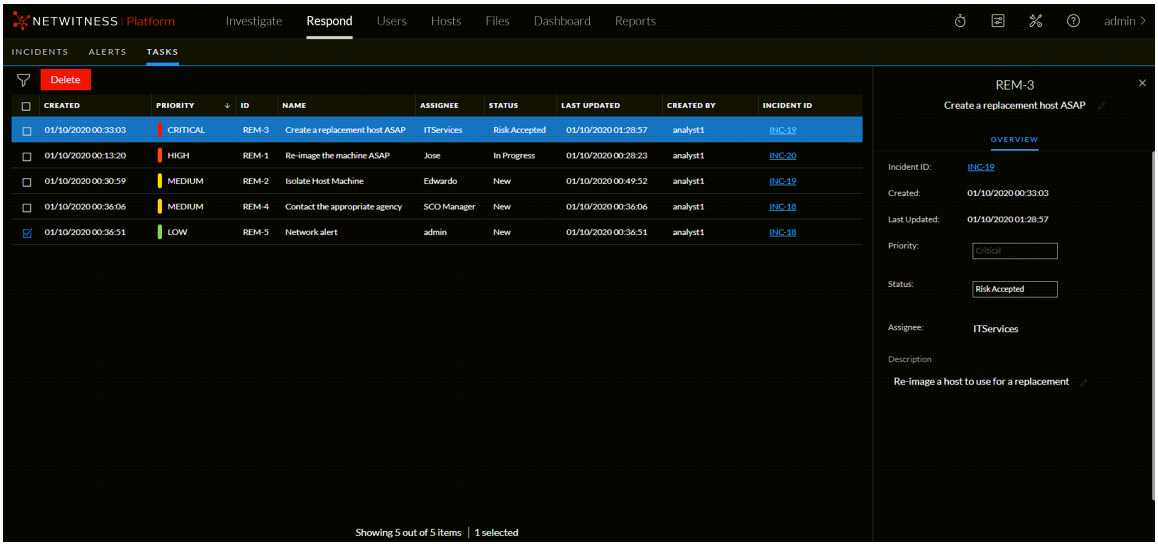
- Incident Details View
- Escalate or Remediate the Incident

Quick Look

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



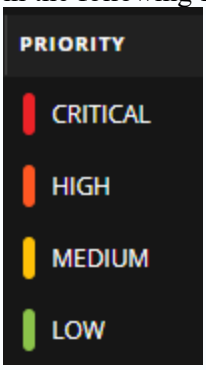
The Tasks List view consists of a Filters panel, a Tasks List, and a Task Overview panel. The following figure shows the Tasks List and the Overview panel.



Tasks List

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

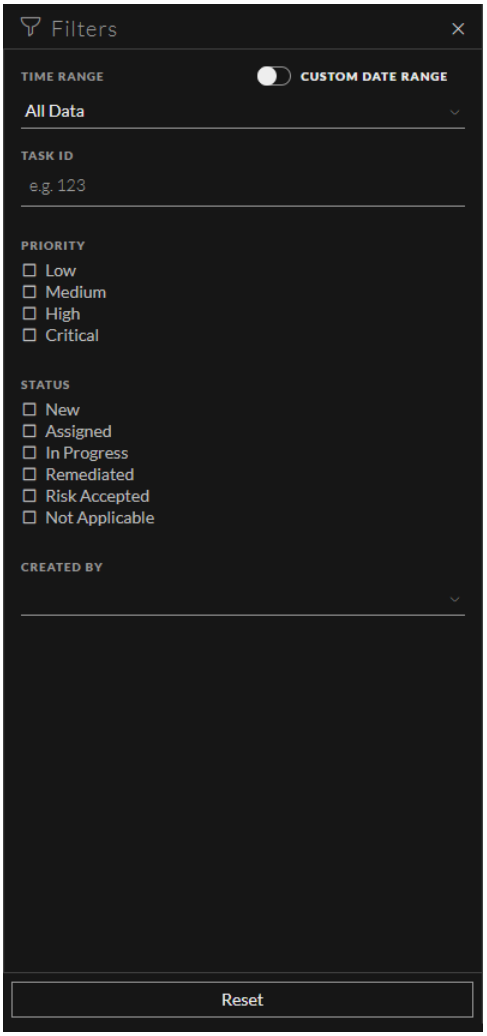
Column	Description
	Enables you to select one or more tasks to modify or delete. Users with the appropriate permissions can make bulk updates and delete tasks, such as SOC Managers. For example, an SOC Manager may want to assign multiple tasks to a user at the same time.
Created	Displays the date when the task was created.

Column	Description
Priority	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates **Critical**, orange represents **High** risk, yellow indicates **Medium** risk, and green represents **Low** risk as shown in the following figure: 
ID	Displays the task ID.
Name	Displays the task name.
Assignee	Displays the name of the user assigned to the task.
Status	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
Last Updated	Displays the date and time when the task was last updated.
Created By	Displays the user who created the task.
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**

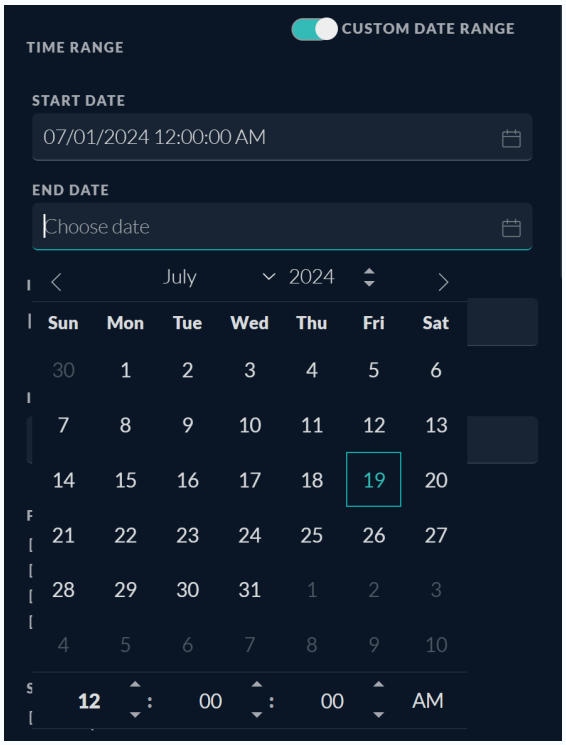
Task Filters Panel

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



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

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

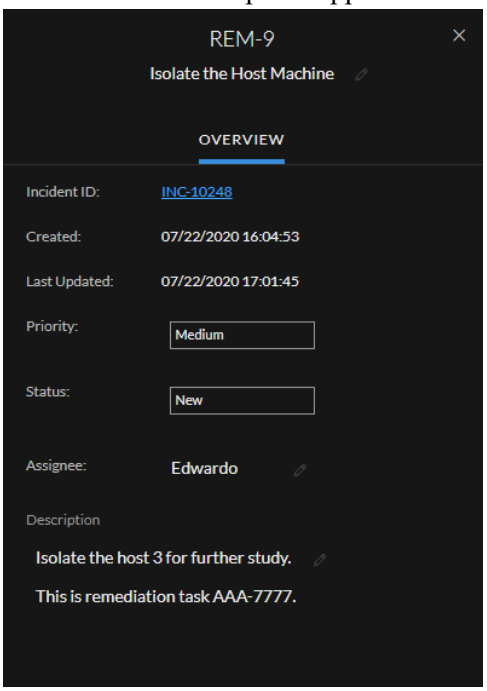
Option	Description
Custom Date Range	You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar. 
Task ID	You can type the Task ID for a task that you would like to locate, for example REM-123.
Priority	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. For example: If you select Critical, the Tasks list shows only the tasks with a priority set to Critical.
Status	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. For example: If you select Assigned, the Tasks panel shows only the tasks that are assigned to users.
Created By	You can select the user who created the tasks that you would like to view. For example, if you only want to view the tasks created by Edwardo, select Edwardo from the CREATED BY drop-down list. If you want to view tasks regardless of the person who created the task, do not make a selection under CREATED BY.
Reset Filters	Removes your filter selections.

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

Task Overview Panel

To access the Task Overview panel:

1. Go to **Respond > Tasks**.
2. In the Task list, click the task that you want to view.
   The Task Overview panel appears to the right of the Tasks list.



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

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

Whitelists List View

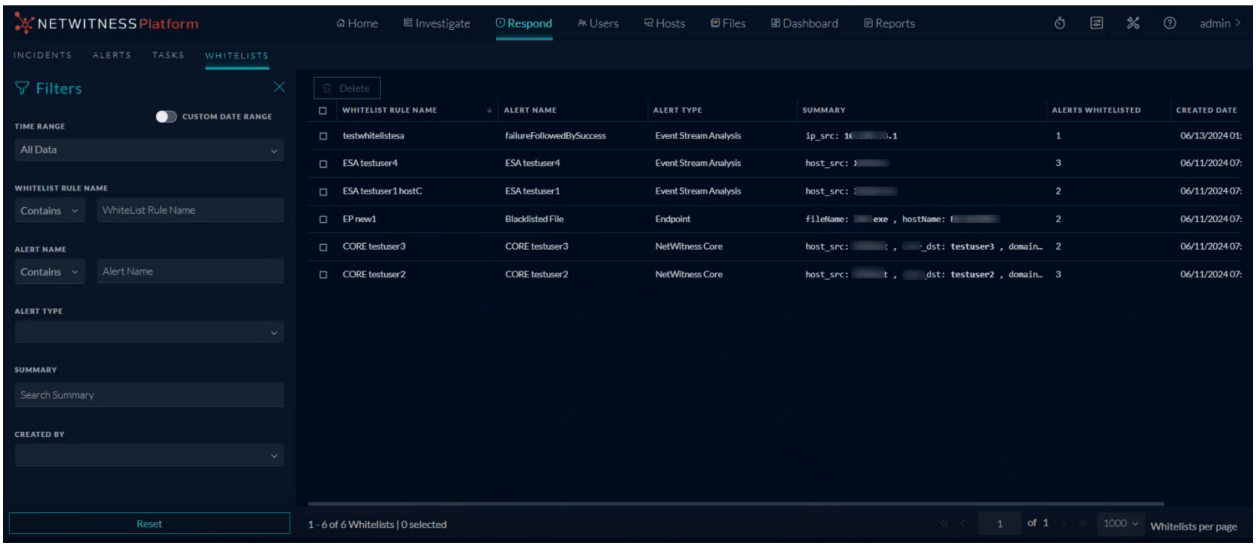
The Whitelists List view (**Respond** > **Whitelists**) enables you to view all the Endpoint and Insight Whitelists with the Rule Name, Creation Date, and the Summary associated with the respective Whitelisted Endpoint and Insight Alerts.

Related Topics

- Whitelist Alerts
- Whitelist Insight Alerts from Respond View

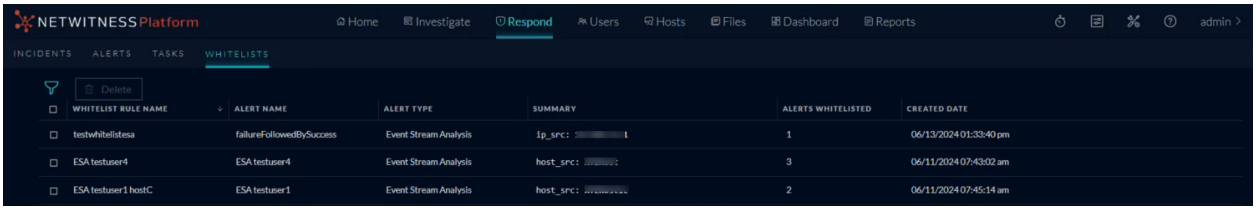
Quick Look

To access the Whitelists List view, go to **Respond > Whitelists**. The Whitelists List view consists of the Whitelists List and a **Filters** panel.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
INCIDENTS
ALERTS
TASKS
WHITELISTS
Filters
CUSTOM DATE RANGE
TIME RANGE
All Data
WHITELIST RULE NAME
Contains
WhiteList Rule Name
ALERT NAME
Contains
Alert Name
ALERT TYPE
SUMMARY
Search Summary
CREATED BY
Reset
Delete
WHITELIST RULE NAME
ALERT NAME
ALERT TYPE
SUMMARY
ALERTS WHITELISTED
CREATED DATE
testwhitelistesa
failureFollowedBySuccess
Event Stream Analysis
1
06/13/2024 01:
ESA testuser4
ESA testuser4
Event Stream Analysis
3
06/11/2024 07:
ESA testuser1 hostC
ESA testuser1
Event Stream Analysis
2
06/11/2024 07:
EP new1
Blacklisted File
Endpoint
2
06/11/2024 07:
CORE testuser3
CORE testuser3
NetWitness Core
2
06/11/2024 07:
CORE testuser2
CORE testuser2
NetWitness Core
3
06/11/2024 07:
1 - 6 of 6 Whitelists | 0 selected
1
of 1
1000
Whitelists per page

Whitelists List

The Whitelists List displays all the Whitelists in the NetWitness Platform. You can filter this list to view only the Whitelists of interest.



The following table describes the columns in the Whitelists List.

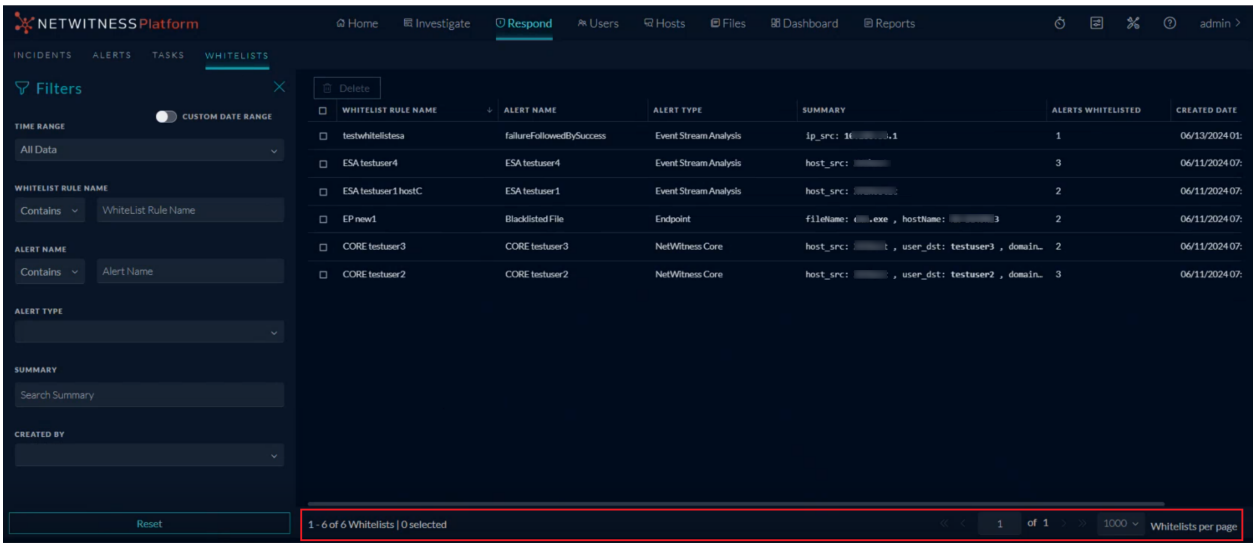
Columns	Description
Whitelist Rule Name	Displays the name of the Whitelist you provided during the whitelisting of the selected alert.
Alert Name	Displays the rule name associated with the whitelisted alert.
Alert Type	Displays the rule name associated with the whitelisted alert.
Summary	Displays the details of the entities or values selected during the whitelisting of the selected alert. For Example: **File name: cmd.exe, Host name: win34.**
Alerts Whitelisted	Displays the number of number of alerts suppressed after the creation of Whitelist.
Created Date	Displays the Whitelist creation date and time.

The following parameters are displayed at the bottom of the list.

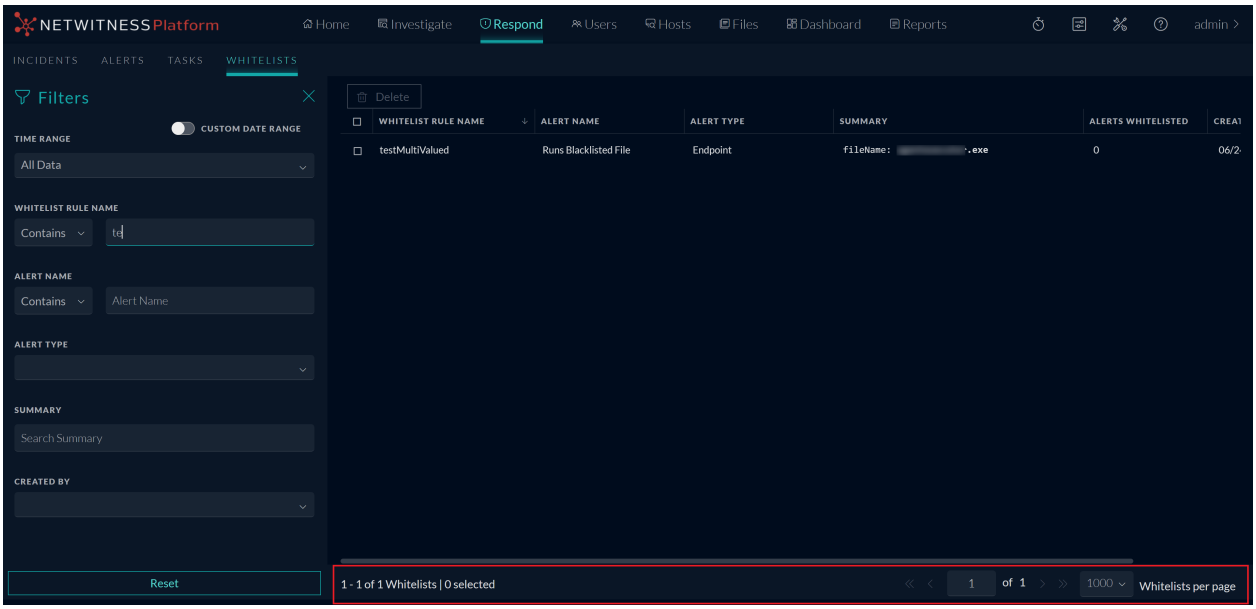
- The count of the Whitelists displayed on the current page.
- The total number of Whitelists created.
- The number of Whitelists selected in the list.
- The current page number.
- Total number of pages available.
- The maximum number of Whitelists displayed in each page.

The values of the above mentioned parameters vary depending upon the filters you apply.

For example, consider the existing count of the Whitelists displayed on page **1** is **1 - 3** and the total number of Whitelists created is **3**.

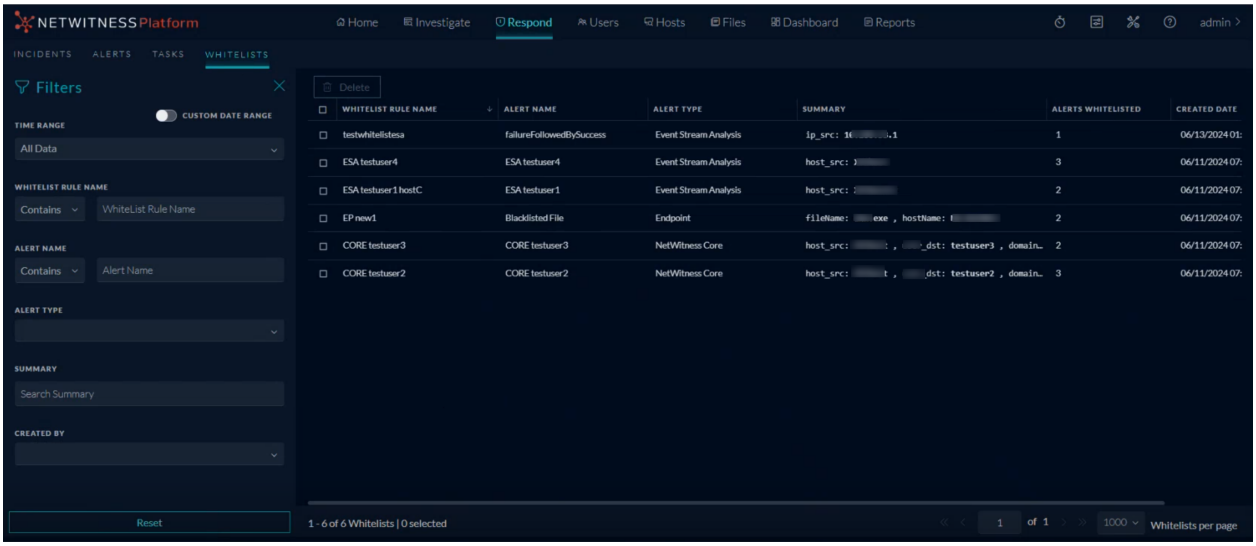


After entering the Whitelist name (completely or partially) in the **Filters** panel and filtering the required Whitelist, the count of the Whitelists displayed on page **1** changes to **1 - 1** and the total number of Whitelists created is displayed as **1** since only 1 Whitelist matches the filter applied.



Whitelists Filters Panel

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



You can filter the Whitelists based on the following parameters.

- Time Range
- Whitelist Rule Name
- Alert Name
- Aler Type
- Summary
- Created By

The following table lists all the fields displayed in the **Filters** panel.

Fields	Description
Time Range	Allows you to select the required time duration and view the Whitelists created in the time duration selected. **Note:** Turn On the **Custom Date Range** Toggle to select a custom date range of your choice.
Whitelist Rule Name	Allows you to enter the name of required Whitelist.
Alert Name	Allows you to enter the name of the rule associated with the Whitelists created.
Alert Type	Allows you to select the alert type: ESA, Endpoint, NetWitness Core, and Insights.

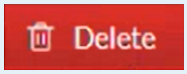
Fields	Description
Summary	Allows you to enter the complete value or a part of the value associated with the required Whitelist. For example: **cmd.exe** or **win34** or **analyst1**.
Created By	Allows you to filter the Whitelists on the basis of the user who created them.

You can click **Reset** at the bottom of the **Filters** panel to remove the filters applied.

When you navigate away from the **Filters** panel, the Whitelists List view retains your filter selections.

Toolbar Actions

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

Option	Description
	Select this option and access the **Filters** panel to filter the required Whitelists.
	Select this option to delete the selected Whitelist.

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 *Context Hub Configuration Guide*.
Administrators	Import or export a list for Context Hub.	See "Import or Export Lists for Context Hub" in the *Context Hub Configuration Guide*.

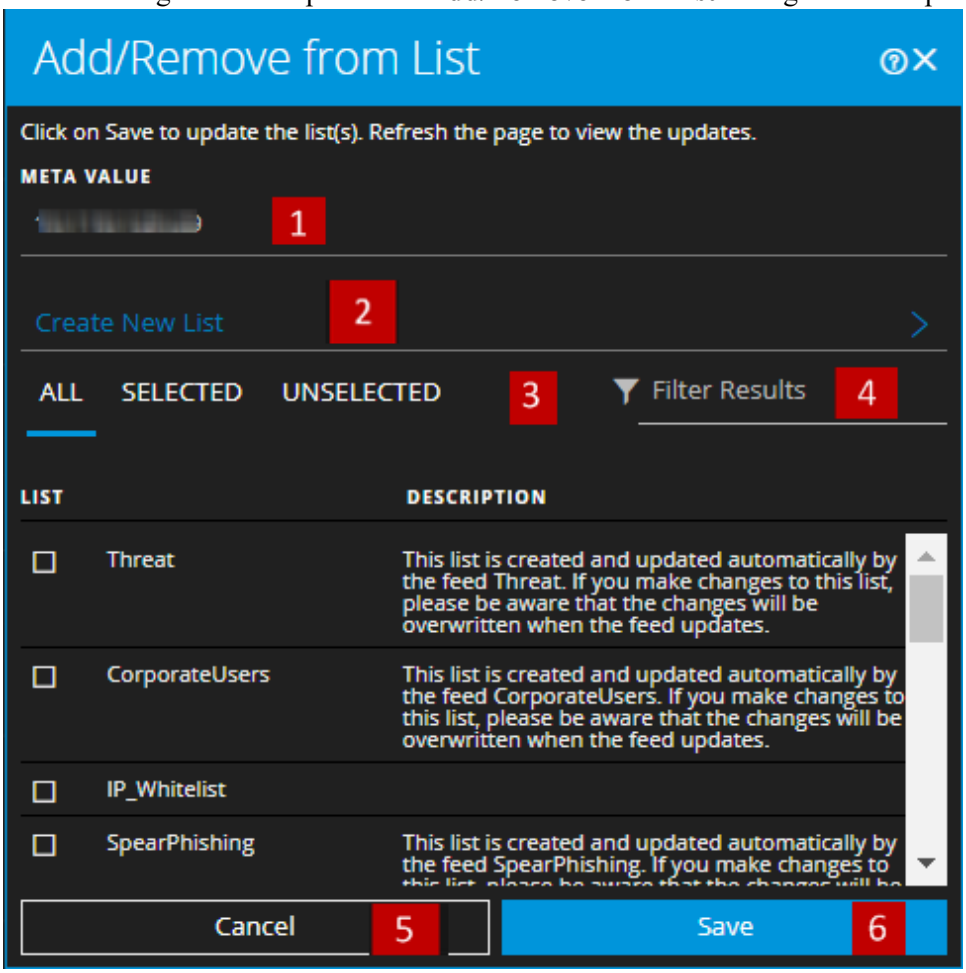
Related Topics

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

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

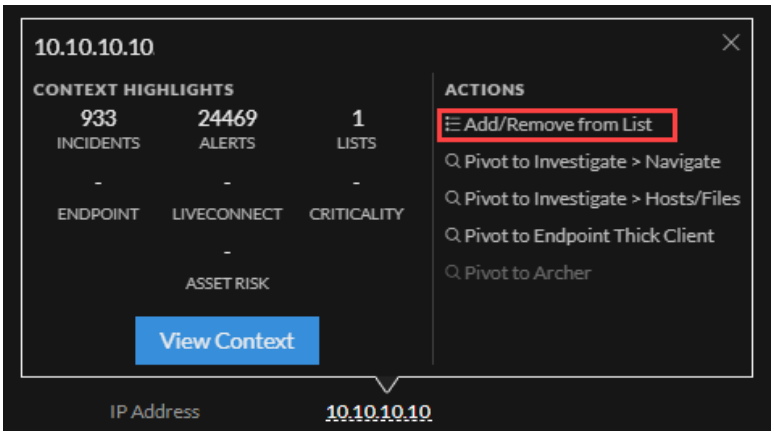
Quick Look

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

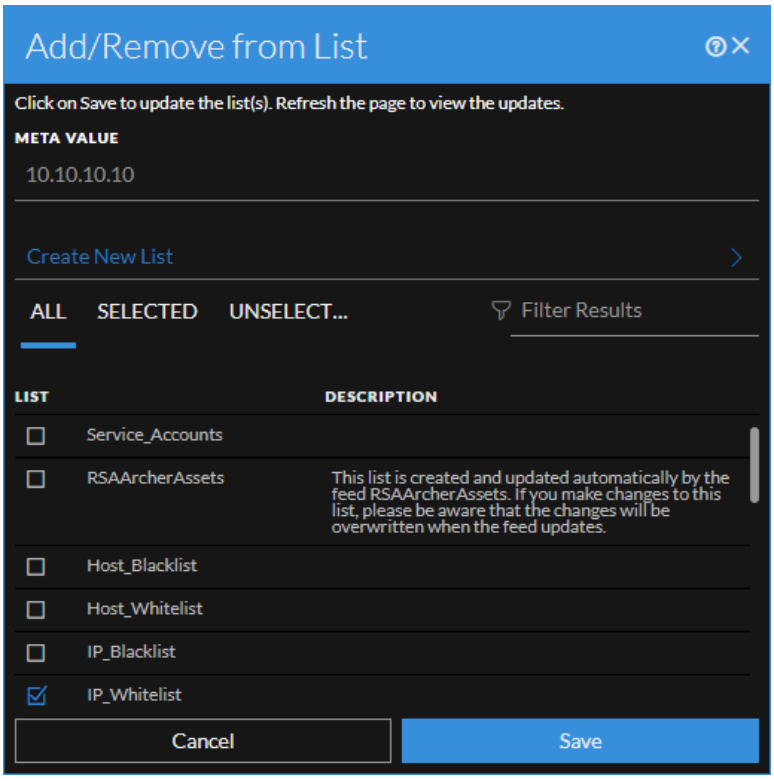


1 Entities or meta values to be added or removed.
2 Create a new list using the selected meta values.
3 Select any of the tabs: All, Selected, or Unselected.
4 Search using the list name or description.
5 Cancel the action.
6 Save to update lists or create a new list.

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 a 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.

Note: The **contexthub-server.contextlookup.read** permission is enabled only for Administrators, Analysts, Malware Analysts, SOC Managers and Respond Administrators. Administrators can enable this permission for other roles in the **Respond** view to view context lookups for meta values and perform the Add/Remove from List actions. For more information, see the "Role Permissions" topic in the *System Security and User Management Guide*.

What do you want to do?

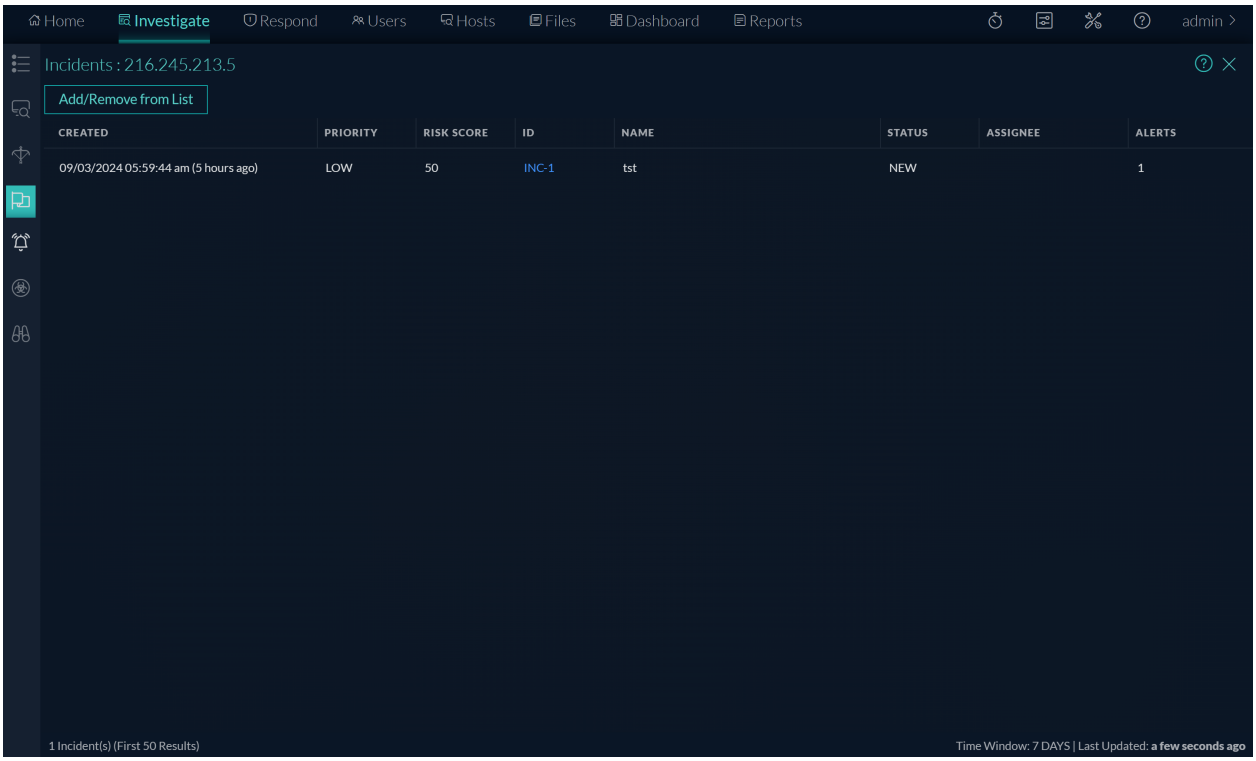
Role	I want to ...	Show me how
Incident Responders, Analysts, Threat Hunters	Navigate to the Context Lookup panel.	From the Incident Details view, see View Contextual Information. From the Alert Details view, see View Contextual Information.
Incident Responders, Analysts, Threat Hunters	Understand the 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 *Context Hub Configuration Guide*.
Administrator	Configure Context Hub settings.	See "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.

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, Incidents, Alerts, and REST API. The following figure shows the Context Lookup panel for a selected entity in the Incident Details view.



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

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

Tab	Description	Supported Entities
 (Incidents)	Displays the list of incidents associated with the selected entity or meta value. The result is sorted by newest incidents to oldest incidents.	All entities
 (Alerts)	Displays the list of alerts associated with the selected entity or meta value. The result is sorted by newest alerts to oldest alerts.	All entities
 (File Reputation)	Displays file reputation status for Filehash entities.	Filehash entities
 TI	Displays information for STIX data sources.	IP address, email address, domain, filename, URL's, and file hash. **Note:** The context lookup for email address and URL will be displayed only if these metas are mapped. Navigate to  (Admin) > System > Investigation > Context Lookup.
 REST API	Displays the list of REST APIs (enabled in Context Hub) associated with selected the entity.	All 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.

Field	Description
Name	The name of the list (defined while creating the list).
Description	The description of the list (defined while creating the list).
Header	Displays the metas available for the list.
Value	Displays the values for each meta in the list.
Author	The owner who created the list.
Created	The date when the list was created.
Updated	The date when the list was last updated or modified.
Count	The number of lists in which the selected entity or meta value is available.
Time Window	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.

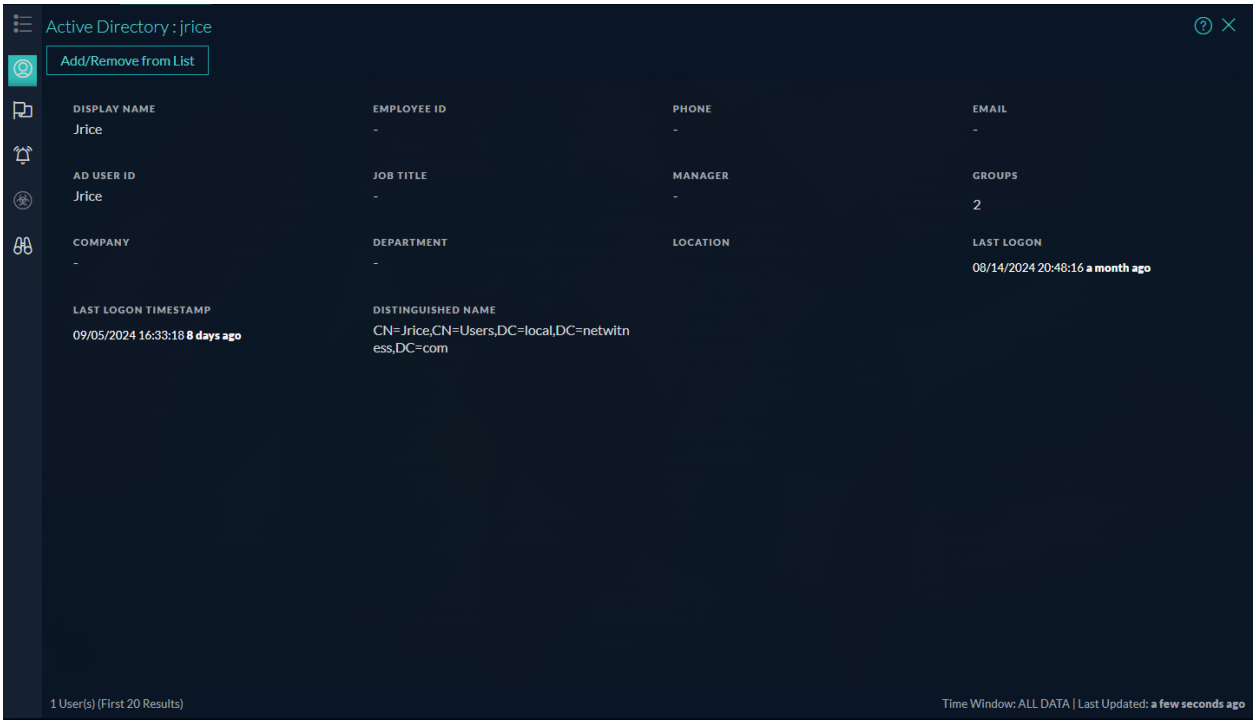
Field	Description
Criticality Rating	The device operational criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High.
Risk Rating	The calculated risk rating for the device based on the most recent assessment and 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.
Internal 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.
Facility	Links to records in the Facilities application that are related to this device.

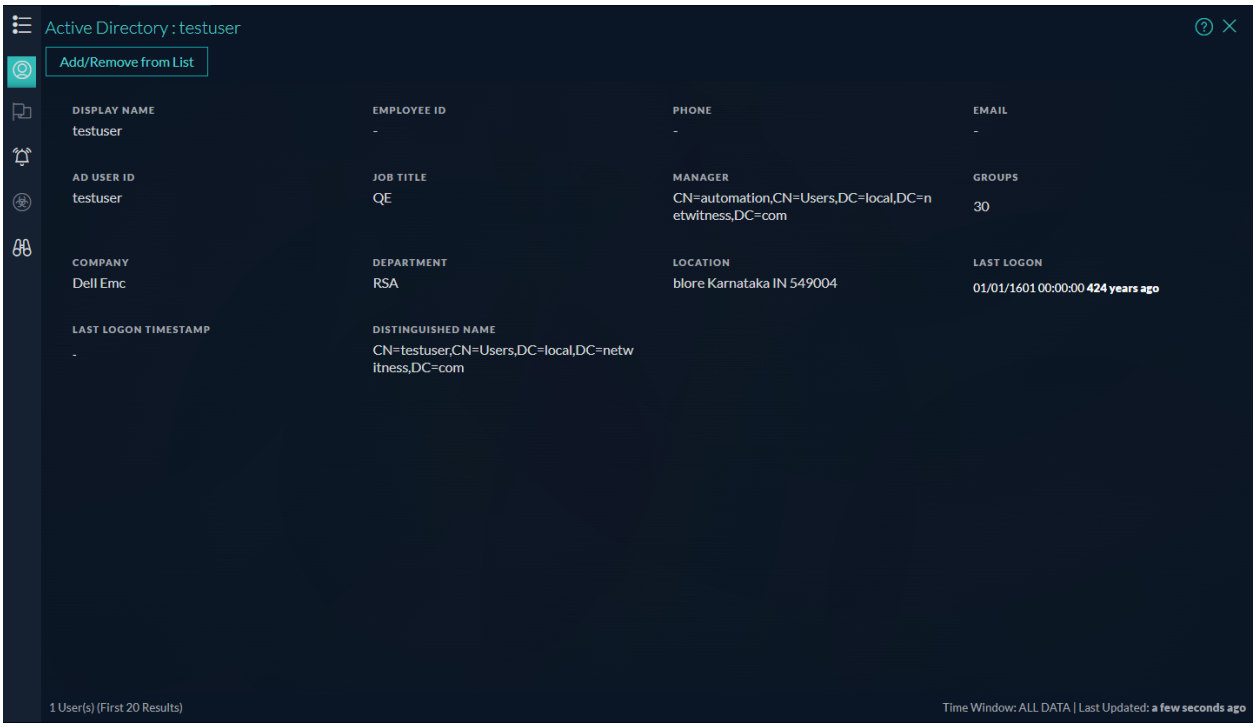
Field	Description
Business Unit	Links to records in the Business Unit application that are related to this device. For more than three business unit values, you can hover over the field to view the values.
Device Owner	The person who is responsible for the device and receives read and update rights of 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, Facility, Internal 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

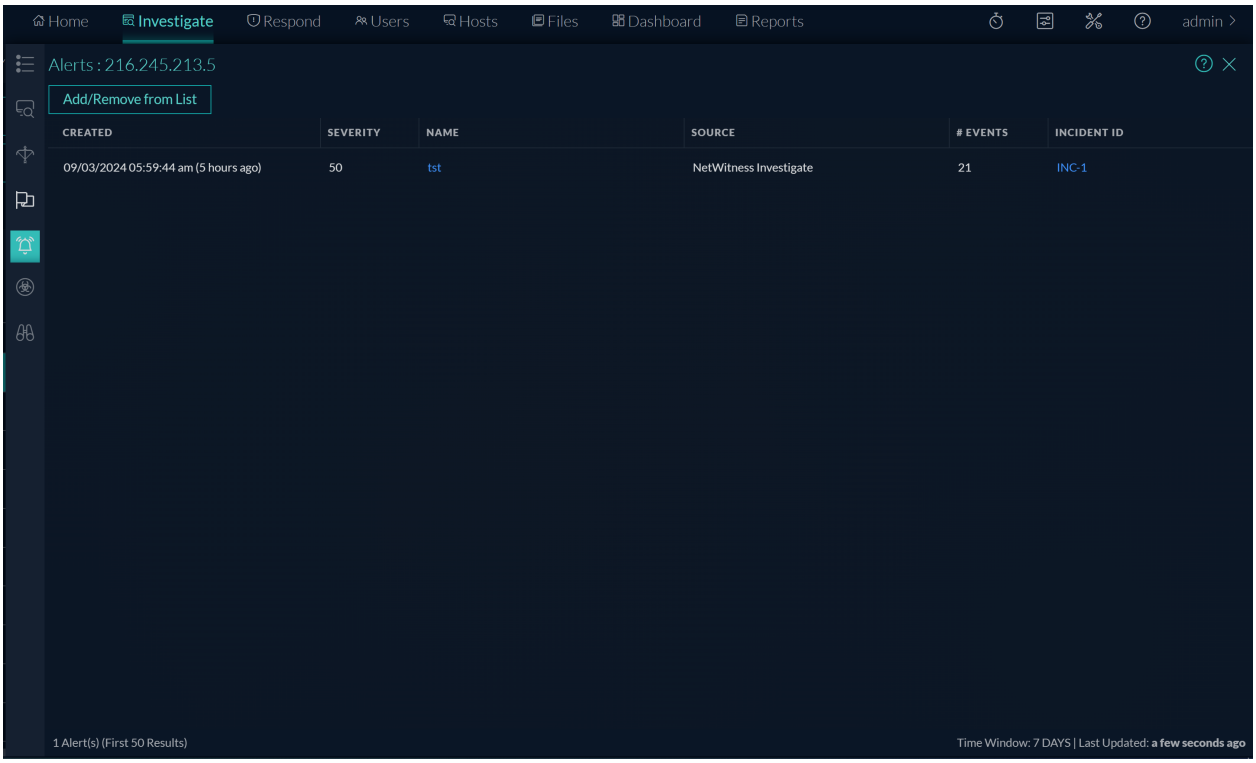
The following information is displayed for Active Directory.

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.
Department	The department name to which the user belongs within the organization.

Field	Description
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.

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.



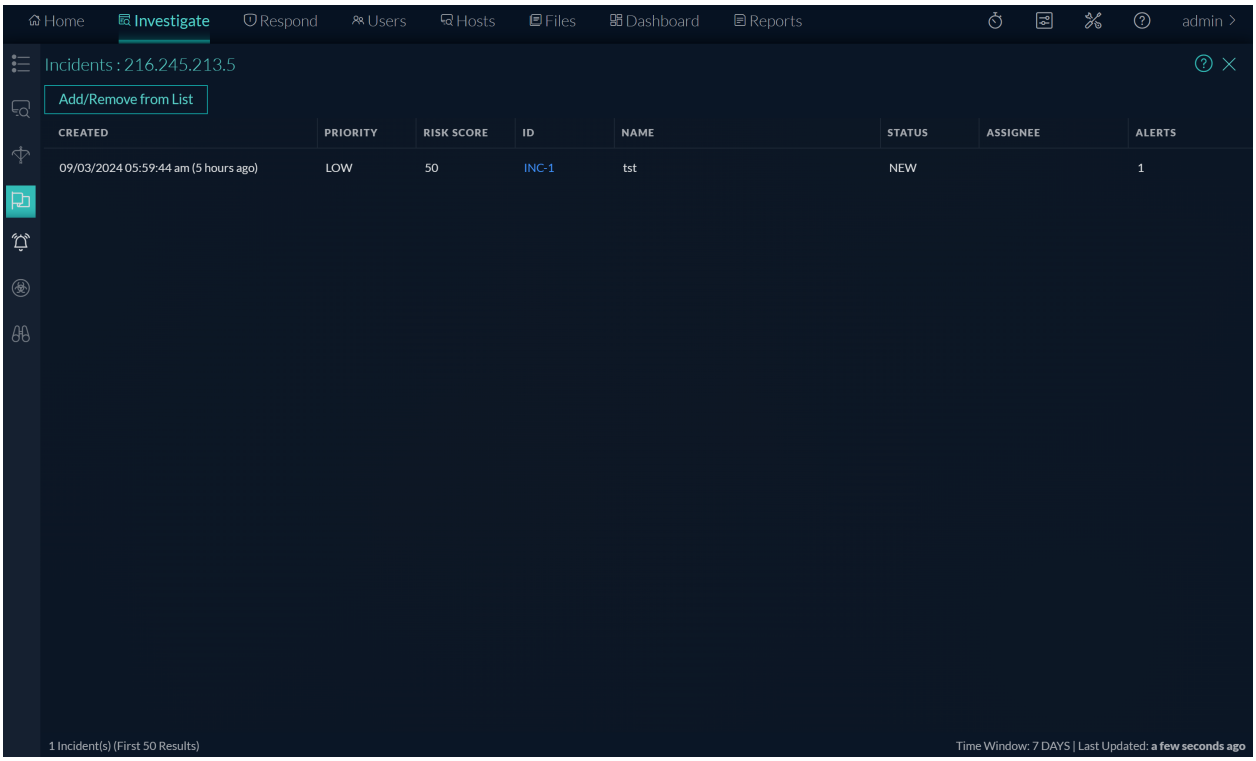
The following information is displayed in the Context Lookup panel for Alerts.

Field	Description
Created	The date and time when the alert was created.

Field	Description
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 *Context Hub Configuration Guide*.
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.

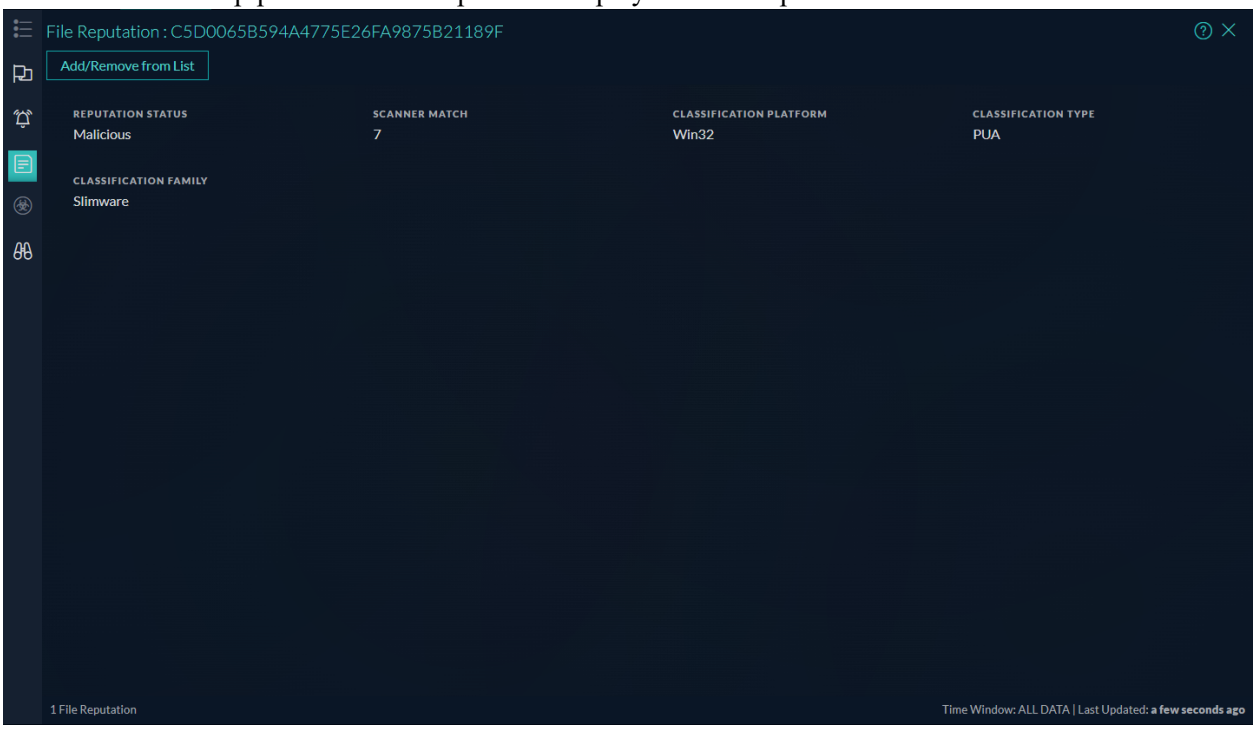


The following information is displayed in the Context Lookup panel for Incidents.

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 *Context Hub Configuration Guide*.
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.

File Reputation Tab

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

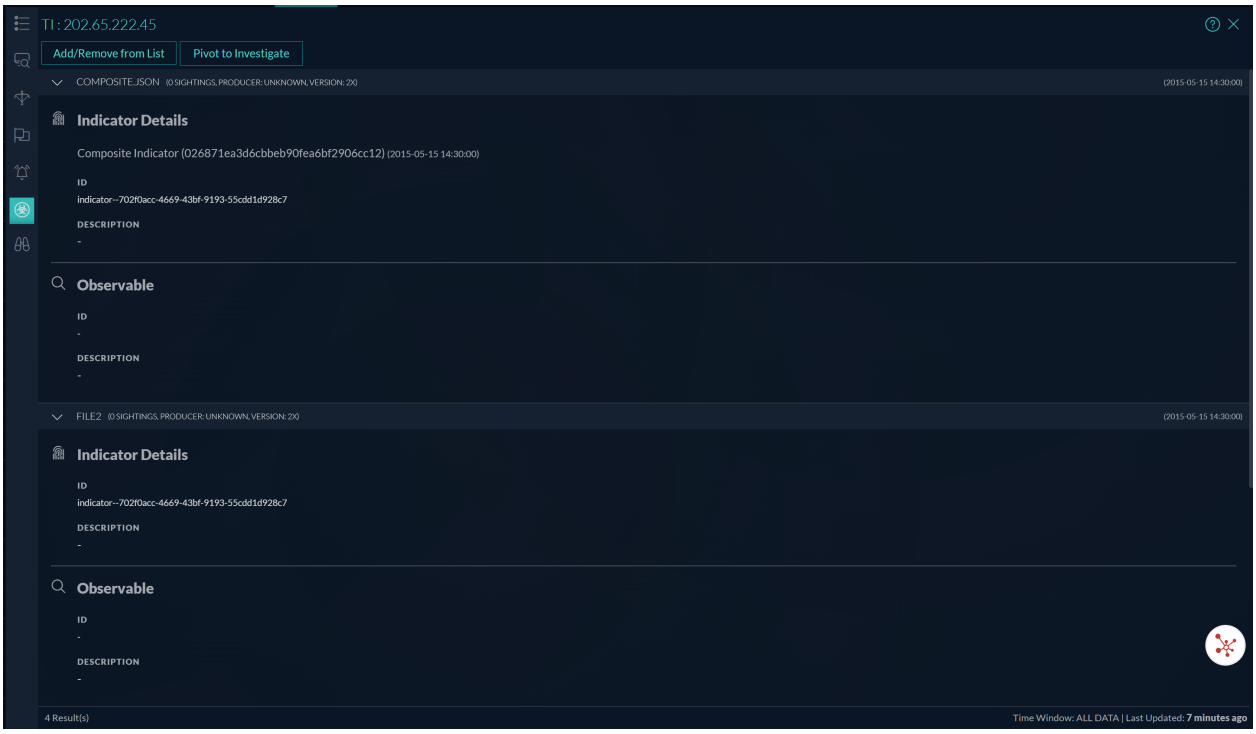


Field	Description
Reputation Status	Reputation Status of filehash. For more information about reputation status, see "View Reputation of files" in the *UEBA User Guide*.
Scanner Match	Number of scanners that detected malware or suspicious activity in the last scan.
Classification Platform	Classification 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.

TI Tab

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

Note: From NetWitness version 12.5 or later, analysts can perform context lookups on indicators that uses STIX V2 (2.0 and 2.1) standards to gain more threat context and enhance their investigations.



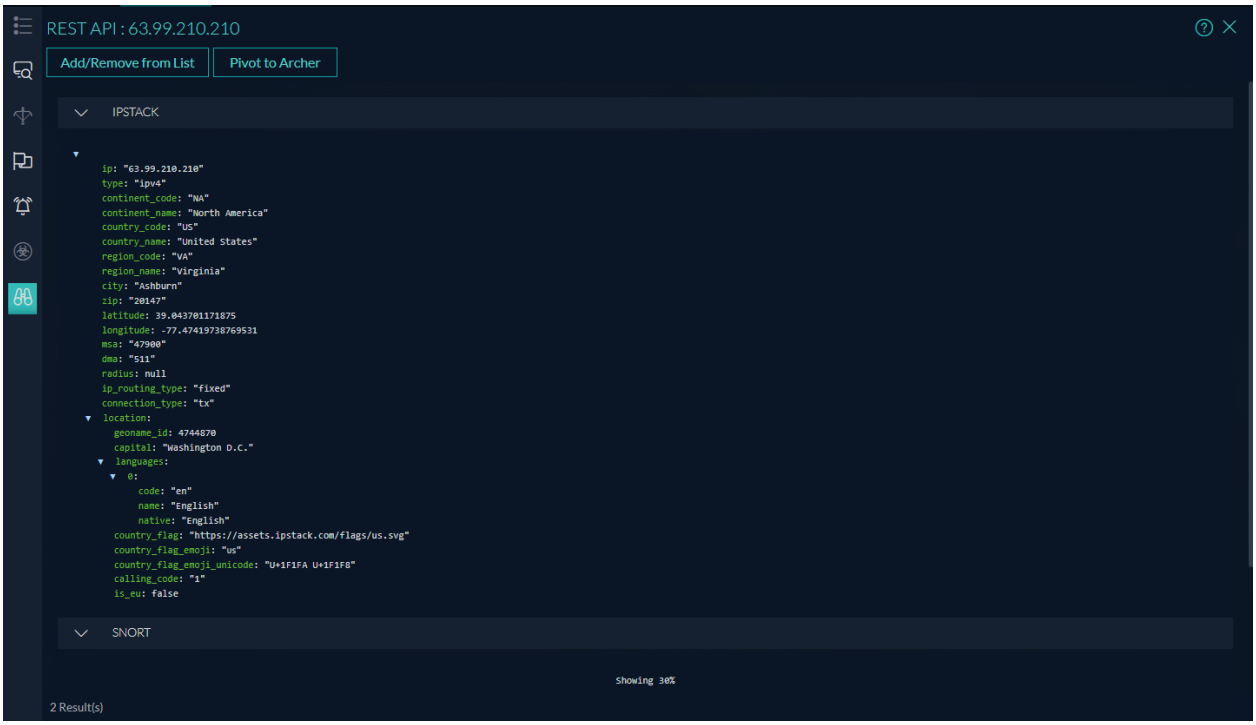
Field	Description
Data Source name	Displays the STIX data source name from where the data is retrieved.
Timestamp	The time when the event was created.
Indicator Details	Indicator Title: Displays the details that contains a pattern that can be used to detect suspicious or malicious cyber activity. ID: Displays the ID of the selected indicator. Produced by: Displays the user role who requested for the STIX data. Description: Displays details about the selected IP address which are being watch listed.
Observable	Observable Title: Displays and conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs). ID: Displays the ID of the selected observable.
(Optional) SightingsREST	Sightings Title: Displays the name of the sighting source. Confidence: Displays the criticality of the sighting. Reference: Displays the reference URL of the sighting source.

REST API Tab

The Context Lookup panel for REST API shows HTML or JSON response (based on the response type configured) associated with the selected entity or meta value.

Note: For JSON response type, the fields that are mapped with friendly names (during REST API configuration) are only displayed for context Lookup. If you have not mapped any fields, all fields are displayed for context lookup.

The following figure is an example of the Context Panel for REST API with JSON response:



The following figure is an example of the Context Panel for REST API with HTML response: