NetWitness® Platform XDR

Version 12.1.0.0

Malware Analysis User Guide

NETWITNESS

Platform XDR

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.

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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

October, 2022

Contents

Malware Analysis Functions

NetWitness Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows portable executable (PE), PDF, and MS Office) to assess the likelihood that a file is malicious.

Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- Network Session Analysis (network)

- Static File Analysis (static)

- Dynamic File Analysis (sandbox)

- Security Community Analysis (community)

Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language, which allows malware researchers to identify and classify malware samples. This allows IOC authors to add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live. These YARA-based IOCs in RSA Live will automatically be downloaded and activated on the subscribed host, to supplement the existing analysis that is performed in each analyzed file.

Malware Analysis also has features that support alerts for Incident Management.

Functional Description

This figure depicts the functional relationship between the Core services (the Decoder, Concentrator, and Broker), the Malware Analysis service, and the NetWitness Server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000
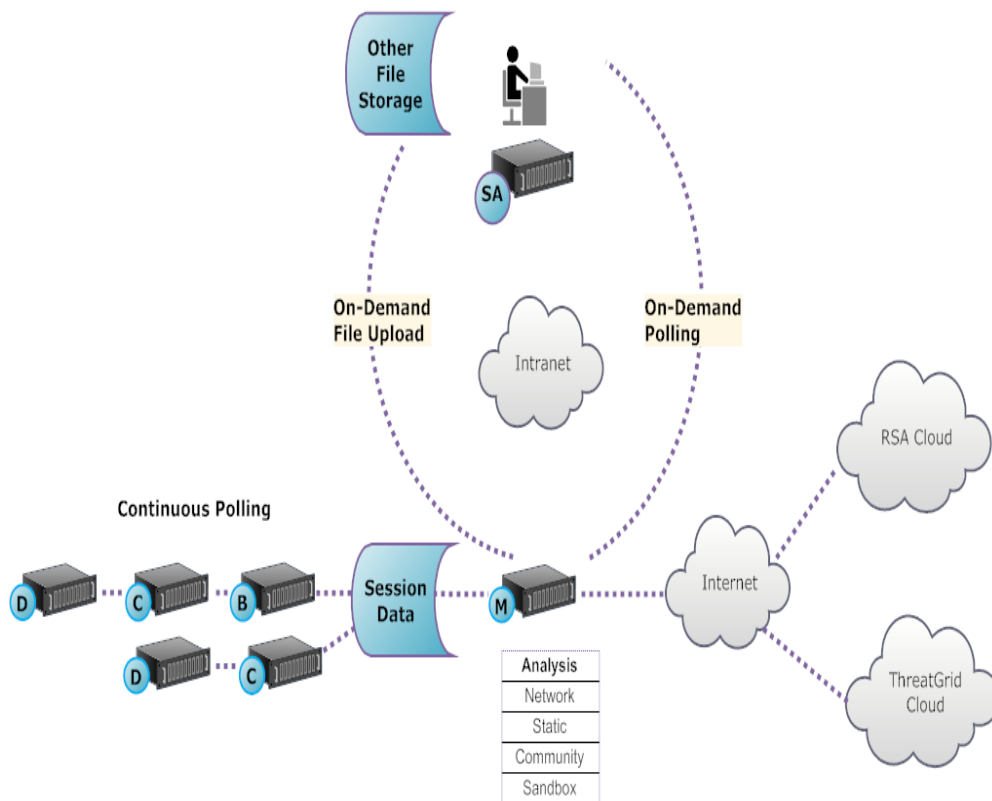
The Malware Analysis service analyzes file objects using any combination of the following methods:

- **Continuous automatic polling of a Concentrator or Broker** to extract sessions identified by a parser as potentially carrying malware content.

- **On-demand polling of a Concentrator or Broker** to extract sessions identified by a malware analyst as potentially carrying malware content.

- **On-demand upload of files** from a user-specified folder.

When automatic polling of a Concentrator or Broker is enabled, the Malware Analysis service continuously extracts and prioritizes executable content, PDF documents, and Microsoft Office documents on your network, directly from data captured and analyzed by your Core service. Because the Malware Analysis service connects to a Concentrator or Broker to extract only those executable files that are flagged as possible malware, the process is both rapid and efficient. This process is continuous and does not require monitoring.

When on-demand polling of a Concentrator or Broker is chosen, the malware analyst uses Investigation to drill into captured data and choose sessions to be analyzed. The Malware Analysis service uses this information to automatically poll the Concentrator or Broker and to download the specified sessions for analysis.

On-demand upload of files provides a method for the analyst to review files captured external to the Core infrastructure. The malware chooses a folder location and identify one or more files to be uploaded and analyzed by Malware Analysis. These files are analyzed using the same methodology as files automatically extracted from network sessions.

Analysis Method

For the Network analysis, the Malware Analysis service looks for characteristics that seem to deviate from the norm, much as an analyst does. By looking at hundreds to thousands of characteristics and combining the results into a weighted scoring system, legitimate sessions that coincidentally have a few abnormal traits are dismissed, while the actual bad ones are highlighted. A user can learn patterns that indicate anomalous activity in the sessions as indicators that warrant further investigation, Indicators of Compromise.

The Malware Analysis service can perform Static analysis against suspicious objects it finds on the network and determine whether those objects contain malicious code. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. For Sandbox analysis, the services can also push data into major security, information and event management (SIEM) hosts (the ThreatGrid Cloud).

Malware Analysis has a unique method for analysis that is partnered with industry leaders and experts, so their technologies can enrich the Malware Analysis scoring system.

NetWitness Server Access to the Malware Analysis Service

The NetWitness Server is configured to connect to the Malware Analysis service and import tagged data for deeper analysis in Investigation. Access is based on three subscription levels.

- Free subscription: All NetWitness customers have a free subscription, with a free key for ThreatGrid analysis. The Malware Analysis service is rate-limited to 100 file samples per day. The number of samples (within the set of files from above) submitted to the ThreatGrid Cloud for sandbox analysis is limited to 5 per day. If one network session had 100 files in it, customers would hit the rate limit after processing the one network session. If 100 files were manually uploaded, that would cause the rate limit to be reached.

- Standard subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 1000 per day.

- Enterprise subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 5000 per day.

Scoring Method

By default, the Indicators of Compromise (IOC) are tuned to reflect industry best practices. During analysis, the IOCs that trigger cause the score to move upward or downward to indicate the likelihood that the sample is malicious. The tuning of IOCs is exposed in NetWitness so that the malware analyst can choose to override the assigned score or to disable an IOC from being evaluated. The analyst has the flexibility to either use the default tuning, or to completely customize the tuning to specific needs.

YARA-based IOCs are interleaved with the built-in IOCs within each built-in category and are not distinguished from native IOCs. When viewing IOCs in the Service Configuration view, administrators can select YARA from the Module selection list to see a list of YARA rules.

After a session is imported into NetWitness, all of the viewing and analysis capabilities in Investigation are available to further analyze Indicators of Compromise. When viewed in Investigation, YARA IOCs are distinguished from the built-in native IOCs by the tag `Yara rule.`

Deployment

The Malware Analysis service is deployed as a separate RSA Malware Analysis host. The dedicated Malware Analysis host has an on-board Broker which connects to the Core infrastructure (either another Broker or a Concentrator). Prior to this connection, a collection of parsers and feeds must be added to the Decoders that are connected to the Concentrators and Brokers from which the Malware Analysis service pulls data. This allows suspicious data files to be marked for extraction. These files are `malware analysis` tagged content available through the RSA Live content management system.

Malware Scoring Modules

NetWitness Malware Analysis analyzes and scores sessions and the embedded files within these sessions by scoring four categories: Network, Static Analysis, Community, and Sandbox. Each category comprises many individual rules and checks that are used to calculate a score between 1-100. The higher the score, the more likely the session is to be malicious and worthy of more in-depth follow-on investigation.

Malware Analysis can facilitate a historical investigation into events leading up to a network alarm or incident. If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections. You can also modify behavior for each scoring category based on the scoring category or the file type (Windows PE, PDF, and Microsoft Office).

Once you become familiar with data navigation methods, you can explore the data more completely through:

- Searching for specific types of information

- Reviewing specific content in detail.

Category scores for Network, Static Analysis, Community, and Sandbox are maintained and reported independently. When events are viewed based on the independent scores, as long as one category detects malware, it is evident in the Analysis section.

Network

The first category examines each core network session to determine if the delivery of the malware candidates was suspicious. For example, benign software being downloaded from a well-known safe site, using proper ports and protocols, is considered less suspicious than downloading software known to be malicious from a known dubious download site. Sample factors used in the scoring of this criteria set may include sessions that:

- Contain threat feed information

- Connect to well-known bad sites

- Connect to high-risk domains/countries (for example, .cc domain)

- Use well-known protocols on non-standard ports

- Contain obfuscated JavaScript

Static Analysis

The second category analyzes each file in the session for signs of obfuscation in order to predict the likelihood of the file behaving maliciously if allowed to run. For example, software that links to networking libraries is more likely to perform suspicious network activity. Sample factors used in the scoring of this criteria set may include:

- Files found to be XOR encoded

- Files found embedded within non-EXE formats (for example, PE file found embedded in a GIF format)

- Files linking to higher risk import libraries

- Files highly deviating from the PE Format

Community

The third category scores the session and files based on the collective knowledge of the security community. For example, files whose fingerprint/hash is already known to be good or bad by respected anti-virus (AV) vendors is scored accordingly. Files are also scored based on knowledge that a file was delivered from a site known to be good or bad by the security community.

Community scoring also indicates whether the AV on your network flagged the files as malicious. It does not indicate that the resident AV product acted to protect your system.

Sandbox

The fourth category examines the behavior of the software by actually running it in a sandbox environment. By running the software to watch its behavior, a score can be calculated by identifying well-known malicious activity. For example, software that configures itself to autostart on each reboot and make IRC connections would score higher than a file with no known bad behavior.

Conducting Malware Analysis

Analysts can use theNetWitness Malware Analysis service to detect malware in selected data and files.

Analysts who conduct analysis using NetWitness Malware Analysis need to have the appropriate system roles and permissions set up for their user accounts.

The following procedures provide instructions for using Malware Analysis:

- Begin a Malware Analysis Investigation
- Upload Files for Malware Analysis Scanning
- Implement Custom YARA Content
- Configure the Malware Analysis Summary of Events View
- Filter Dashlet Data in the Summary of Events View
- Examine Scan Files and Events in List Form
- View Detailed Malware Analysis of an Event

Begin a Malware Analysis Investigation

You can investigate data that has been scanned, flagged, and rated by Malware Analysis as containing Indicators of Compromise. This includes all types of Malware Analysis scans: continuous mode polling, on-demand polling, and on-demand uploaded files. Continuous mode polling must be enabled when the administrator configures basic settings for the Malware Analysis service.

NetWitness provides several methods of launching a Malware Analysis investigation.

Fastest: Instant Launch from Malware Analysis Dashlets

The fastest way to begin a Malware Analysis investigation is an Instant launch from the NetWitness Dashboard using one of the Malware Analysis dashlets that lists events or files that are likely to contain malware. The dashlets are described as part of the NetWitness Content in Dashlets. From one of these dashlets, you can go directly to the Analysis Results for a specific event that has been listed as worthy of investigation:

- Top Listing of Highly Suspicious Malware

- Top Listing of Possible Zero Day Malware

- Malware with High Confidence IOCs and High Scores Dashlet

On-Demand Polling from a Meta Value in the Navigate View

You can initiate on-demand polling from within an investigation by right-clicking a meta value in the Navigate view, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis (see "Launch a Malware Analysis Scan from the Navigate View" in the *NetWitness Investigate User Guide*).

Investigate a Specific Service

You can also begin a Malware Analysis investigation of a service in the Investigate > Malware Analysis view. For Malware Analysis investigation on a service basis, a service must be specified in the Investigate > Malware Analysis view.

1. Investigate opens the Malware Analysis view with the user-specified default service selected.

2. If no default service is currently specified, a dialog allows you to select the Malware Analysis service to investigate.

3. When a service has been selected in the Malware Analysis view, the Summary of Events for the selected service and continuous scan data for the service is displayed.

This topic provides instructions for all methods of launching a Malware Analysis investigation.

Launch a Malware Investigation from a Malware Analysis Dashlet

A prerequisite for this procedure is that one of the following dashlets must be visible in the NetWitness dashboard or in the Malware Analysis view, and must be populated with listed events or files. If you do not see the dashlets, add them and configure the dashlets.

- Top Listing of Highly Suspicious Malware

- Top Listing of Possible Zero Day Malware

- Malware with High Confidence IOCs and High Scores Dashlet

To launch a Malware Analysis investigation from a dashlet:

1. Log in to NetWitness and look for one of the above dashlets in the Monitor view or in the Malware Analysis view

2. In the dashlet, double-click an event or file for deeper analysis. A detailed analysis of the event in the Events List or the event with which the file in the File List is associated is displayed in the Malware Analysis view.

To learn more about configuring the Malware Analysis dashlets in the Monitor dashboard, see "Dashlets" in the *NetWitness Platform Getting Started Guide*.

To learn about the ways you can configure and filter information in dashlets in the Malware Analysis view, refer to Filter Dashlet Data in the Summary of Events View.

To learn about the actions you can perform in the Analysis Results, refer to View Detailed Malware Analysis of an Event.

Begin a Malware Analysis Investigation (No Default Service)

To begin an investigation with no default service specified:

1. Select **Investigate > Malware Analysis**.

   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel and available scan jobs in the right panel. This scan jobs panel contains the same columns as the Malware Scan Jobs dashlet in the Unified dashboard. In addition, it has a toolbar and View options, which are described in Select a Malware Analysis Service Dialog.
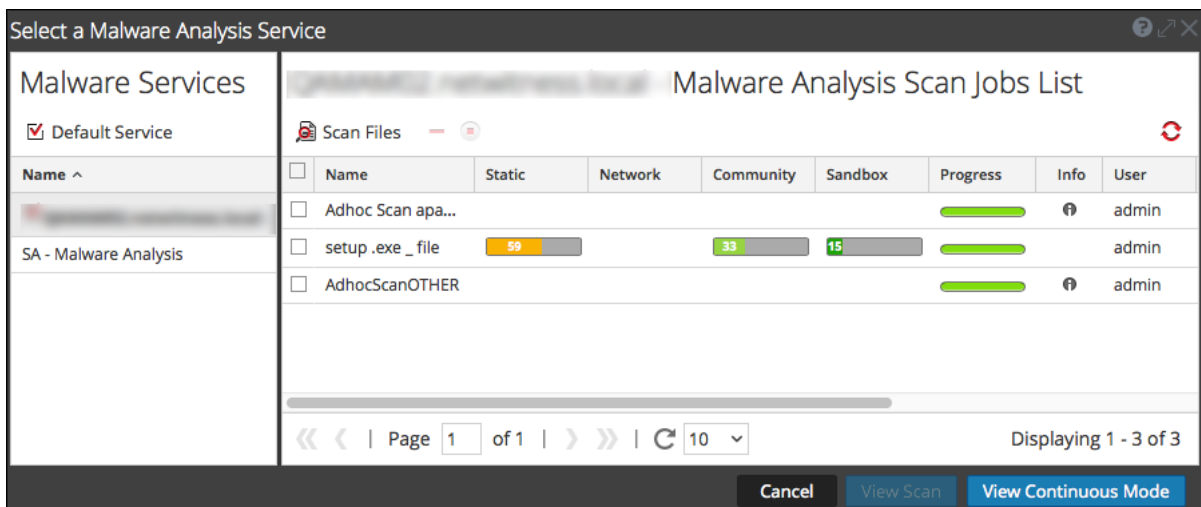
2. In the list of Malware Analysis hosts, select a host and a list of scan jobs is displayed in the right panel. These jobs are created when you scan an event or a file (see Upload Files for Malware Analysis Scanning and "Launch a Malware Analysis Scan from the Navigate View" in the *NetWitness Investigate User Guide*.

3. To begin analyzing a scan, do one of the following:

   a. Select a scan and click **View Scan**.

   b. Click **View Continuous Mode**.

   The Summary of Events for the selected scan is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter Dashlet Data in the

[Summary of Events View](#).
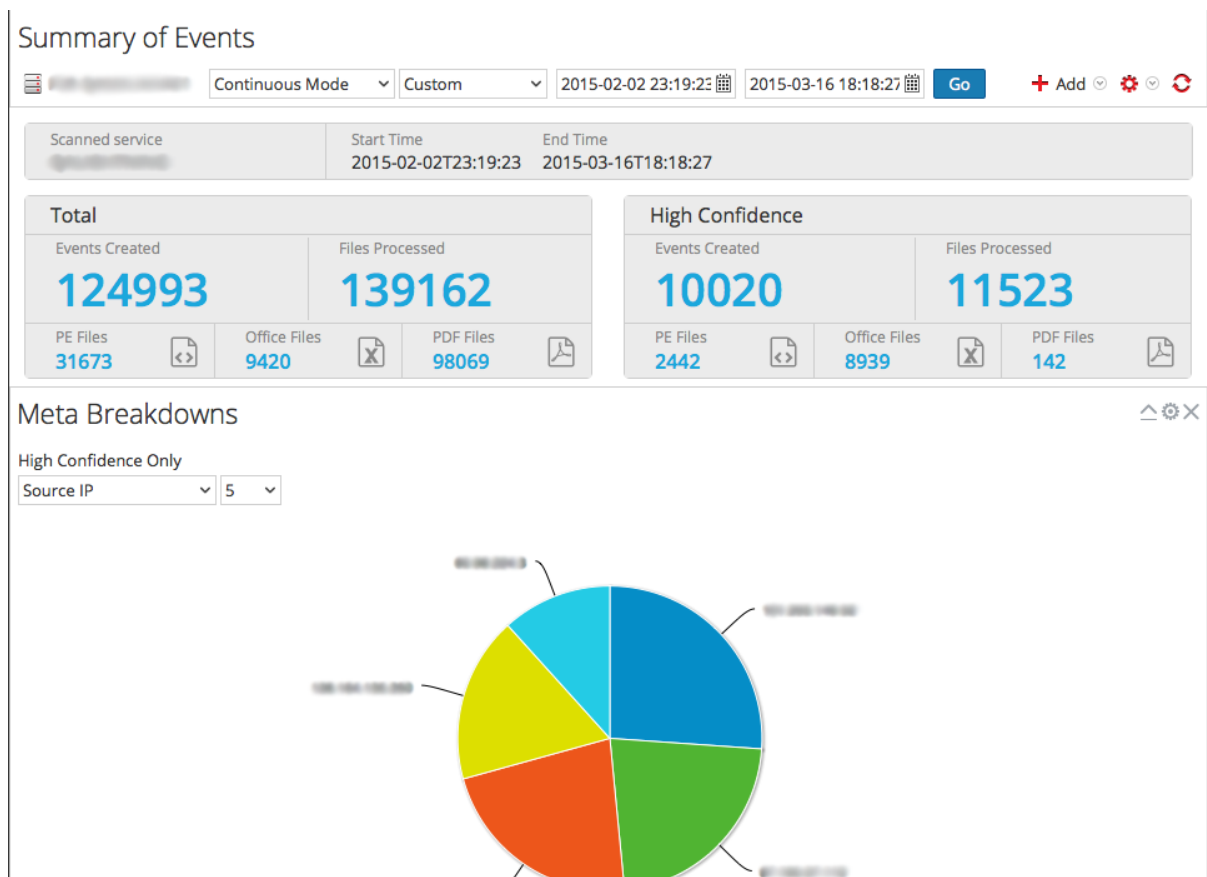
Set or Clear the Default Service

You can set the default service and clear the default service in the Select a Malware Analysis Service dialog.

To set a default service:

1. Click the service name in the Summary of Events toolbar.

    The Select a Malware Analysis Service dialog is displayed.
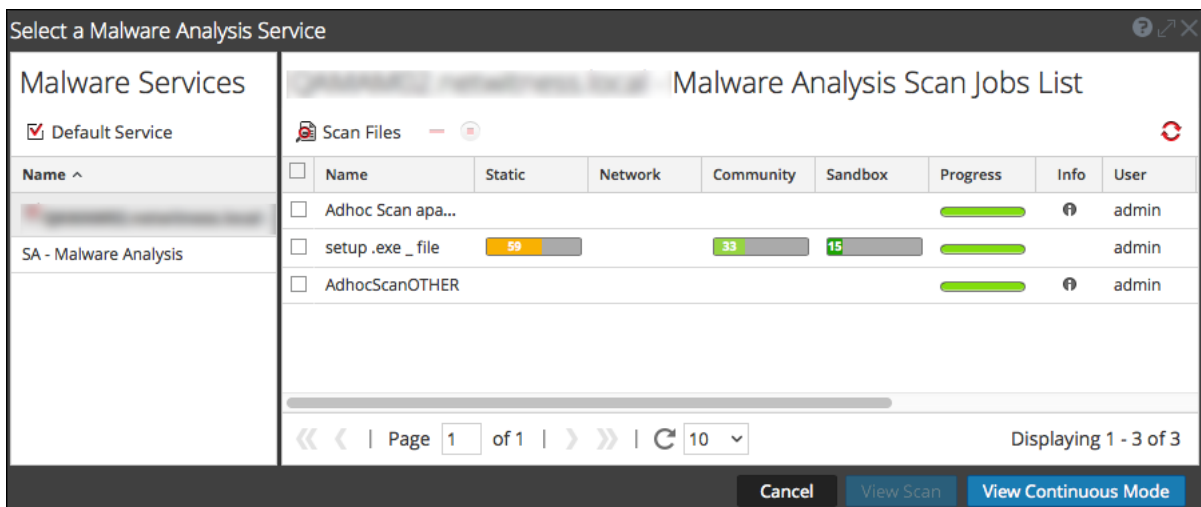
2. Select a service on the list of available Malware services, and click ☑ Default Service.

   The service becomes the default, (indicated by ☑ in front of the host name).

3. To clear the default service, select the default service in the grid, and click ☑ Default Service.

   No default service is set.

Upload and Scan Files

A Malware Analyst with permission to `Initiate Malware Analysis Scan` can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog (see Upload Files for Malware Analysis Scanning. An administrator can upload packet capture files to a Decoder for Malware Analysis in the Services System view as described in "Upload Packet Capture File" in the *Decoder and Log Decoder Configuration Guide*.

Begin an Investigation (Default Service Specified)

To begin an investigation with a default service specified, select **Investigate > Malware Analysis**.

The Summary of Events for a continuous scan of the selected service is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter Dashlet Data in the Summary of Events View.
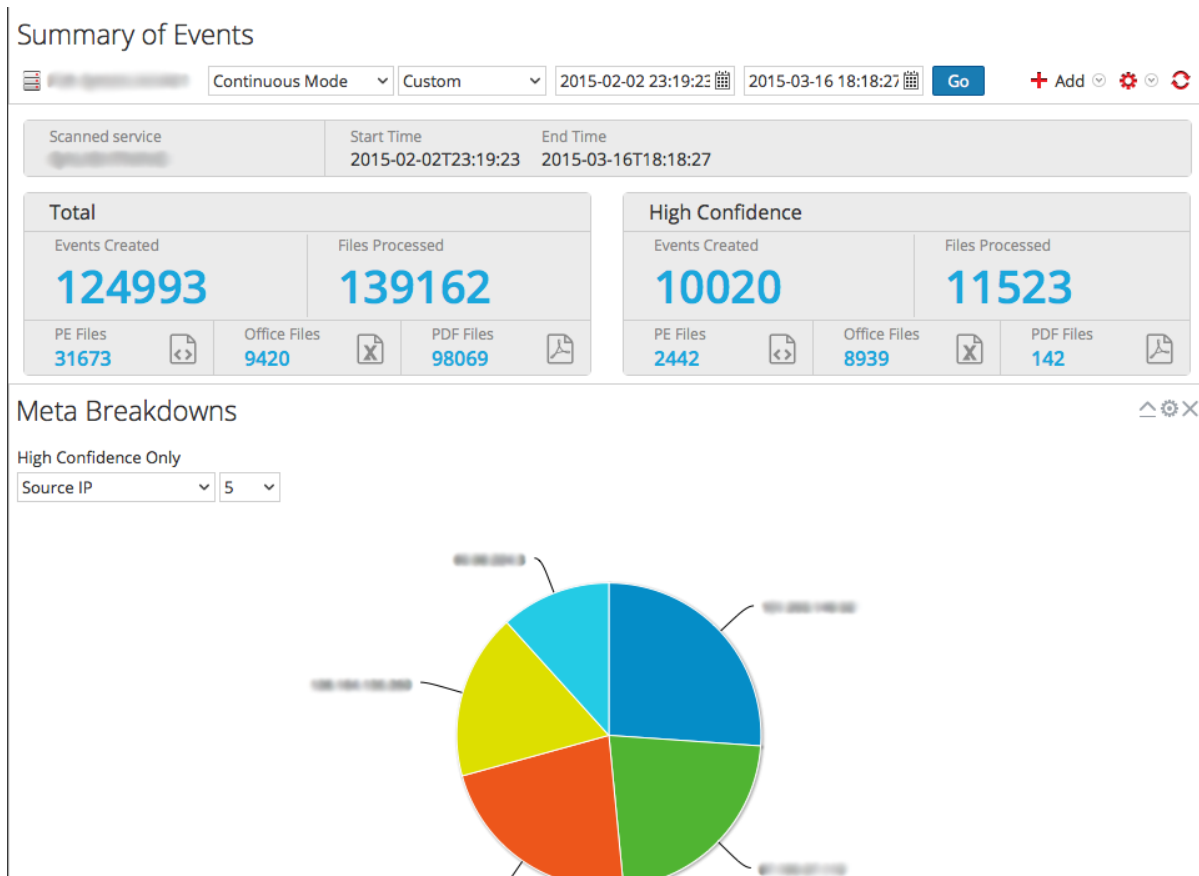
Apply Time Parameters Filter for Results

You can apply a Threshold filter to refresh the results of the chosen dashlets.

1. To select a different time range, select either **Continuous Mode** or a different scan from the toolbar.

   The Malware Summary of Events for the selected scan is displayed.

2. To select a new time range for the scan, click in the range selection list in the toolbar. Ranges available are: Last 5 minutes, Last 10 minutes, Last 15 minutes, Last 30 minutes, Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 5 Days, Early Morning, Morning, Afternoon, Evening, All Day, Yesterday, This Week, Last Week, or Custom.
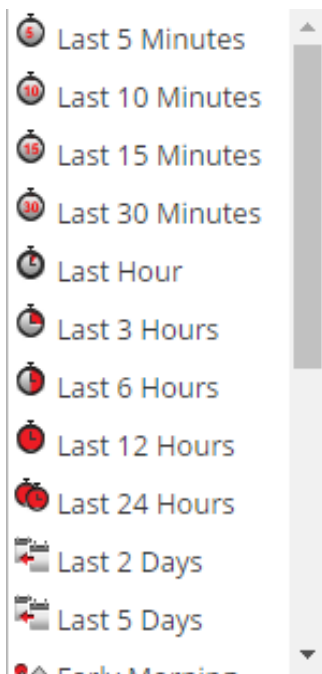
The results are updated immediately.

3. To refresh a continuous mode scan with new data, click ⟳.

Apply a Threshold Filter to Continuous Mode Results

You can apply a new threshold filter to an instance of the Malware with High Confidence IOCs and High Scores dashlet, the Meta Treemap dashlet, the Score Wheel dashlet, and the Event Timeline dashlet.

To customize the scoring applied to the scan, in the toolbar, do the following:

1. Select ⚙ ⌄ > **Apply Threshold Filter**.

   The Apply Threshold Filter dialog is displayed.
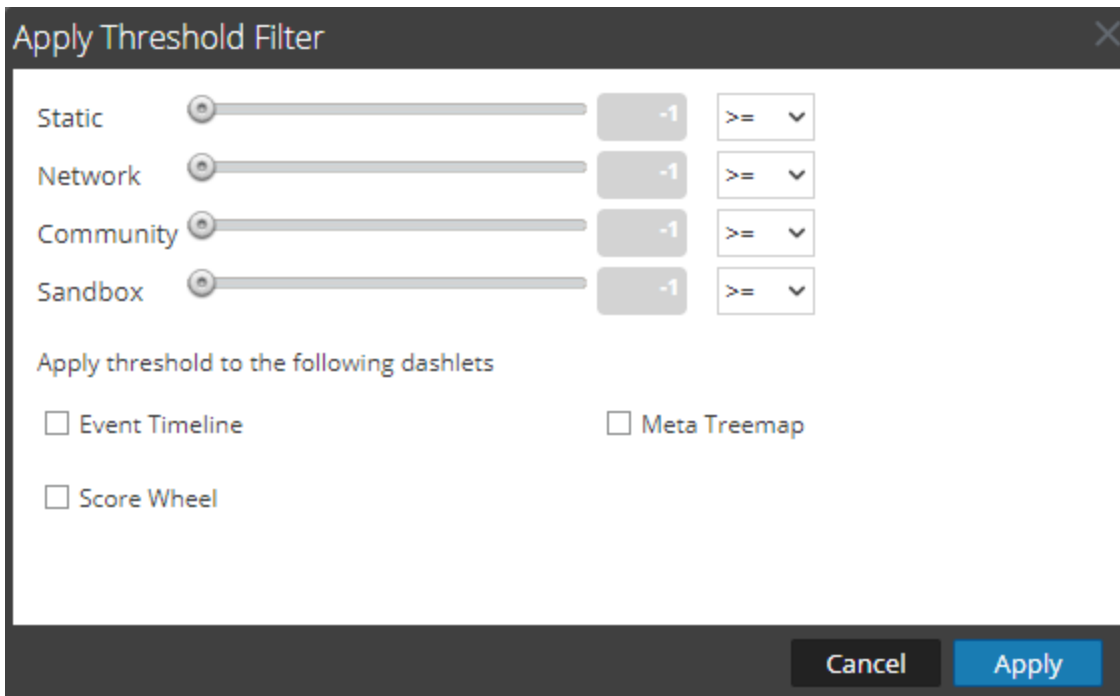
2. If you want to limit the number of events displayed to events that were given a score above a certain number, do the following:

   a. Drag the slider in the Static, Network, Community, and Sandbox slider bars.

   b. To select the dashlets in which the thresholds apply, select the appropriate checkboxes.

   c. Click **Apply**.

Delete or Resubmit an On-Demand Scan with New Bypass Settings

You can delete an on-demand scan or resubmit an on-demand scan with different bypass settings than those specified in the Service Configuration view for a Malware Analysis service.

To delete a scan while viewing an on-demand scan, do the following:

1. Select **Actions > Delete Scan**.

   A dialog asks for confirmation that you want to delete the scan.

2. Click **Yes**.

   The selected scan is deleted.

To apply different bypass settings to the current scan:

1. Select **Actions > Resubmit Scan**.

   The Scan for Malware dialog is displayed.
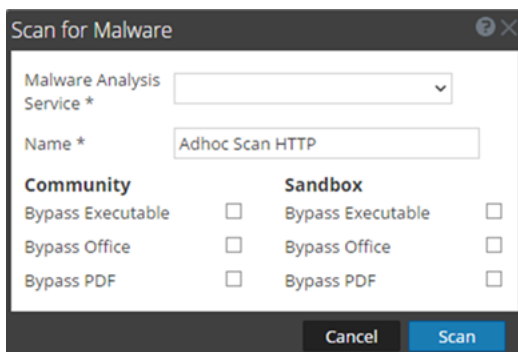
2. Select the bypass settings that you want to use on the new scan, and click **Scan**.

   Malware Analysis resets cache and resubmits the file for a new scan, and the scan jobs are added to the jobs queue.

3. When the job is complete, scroll to the left and select **View**.

   The Malware Summary of Events for the selected scan is displayed.

View the Files List

You can view a list of files for an event from the Malware Analysis Summary of Events and from each of the Visualization charts: Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel.

To view the Files List, do one of the following:

- In the Summary of Events, click on the number of files in the **Total** row or the **High Confidence** row under **Files Processed**, **PE Files**, **Office Files**, or **PDF Files**. The Files List is displayed.

- In any visualization dashlet, click the number next to the **Files** field in the top right corner of the dashlet.

The Files List for the selected drill point is displayed.

From the Files List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files as described in Examine Scan Files and Events in List Form.

To return to the Summary of Events, click **Back to Summary**.

View the Events List

From the Malware Analysis Summary of Events and from each of the visualization charts (Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel), you can select events to view in the Events grid.

To view the Events List, do one of the following:

• In the Summary of Events, click the number of Events Created in the **Total** row or the **High Confidence** row. The Events List is displayed.

• In any visualization dashlet, click the number next to the Events field in the top right corner of the dashlet.

The Events List for the selected time is displayed.

Implement Custom YARA Content

In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language that allows malware researchers to identify and classify malware samples. It makes built-in YARA-based Indicators of Compromise (IOCs) available in Live; these are automatically downloaded and activated on subscribed hosts.

Customers with advanced skills and knowledge can add detection capabilities to Malware Analysis by authoring YARA rules and publishing them in Live or placing YARA rules in a watched folder for the host to consume.

As malware and the threat landscape evolve, it is important to review and examine existing custom rules. Updates are often necessary to incorporate new detection methods. It also updates YARA rules in Live from time to time. To receive updates, you can subscribe to the Blog and Live at http://blogs.rsa.com/feed.

This document provides information to help customers implement custom YARA rules in Malware Analysis.

Prerequisites

The host on which you are adding custom rules must be configured to support authoring of YARA rules as described in "Enable Custom YARA Content" in the *Malware Analysis Configuration Guide*.

YARA Version and Resources

Malware Analysis is packaged with YARA version 1.7 (rev:167). To find out the exact version, you can run `yara -v` on the Malware Analysis host as shown in this example:

```
[root@TESTHOST yara] # yara -v
 yara 1.7 (rev:167)
```

Meta Keys in YARA Rules

Malware Analysis is compliant with other sources of YARA rules, and it also consumes additional meta keys that are specific to Malware Analysis. Each YARA rule is equivalent to an Indicator of Compromise (IOC) within Malware Analysis. The example below illustrates the meta definitions in a rule:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Meta Key	Description
iocName	(Required) This is the name that MA uses as the rule name. It is specific to Malware Analysis and is required to add the rule to the IOC list.

Meta Key	Description
fileType	Specifies the files type. Possible values are: WINDOWS_PE, MS_OFFICE, and PDF. If not specified, the default value is WINDOWS_PE.
score	This value that is added to the static score if the YARA rule is triggered. If not specified, the default value is 10.
ceiling	This is the maximum amount that is added to the static scores when a rule is triggered multiple times in one session. For example, if each time a rule is triggered, 20 points are added to the static, and you do not want more that 40 points added when the rule is triggered more than two times, you can specify a ceiling of 40. If not specified, the default value is 100.
highConfidence	This sets the High Confidence flag, which is set on IOCs when there are high confidence indicators that malware is present. If not specified, the default file value is false.

Note: Refer to the following URL for YARA resources: https://code.google.com/p/yara-project/downloads/list. NetWitness uses YARA 1.7, not YARA 2.0.

YARA Content

Live contains 3 sets of Yara rules:

- PE Packers
- PDF Artifacts
- PE Artifacts

The following figure illustrates YARA content available as YARA rules in NetWitness Live.
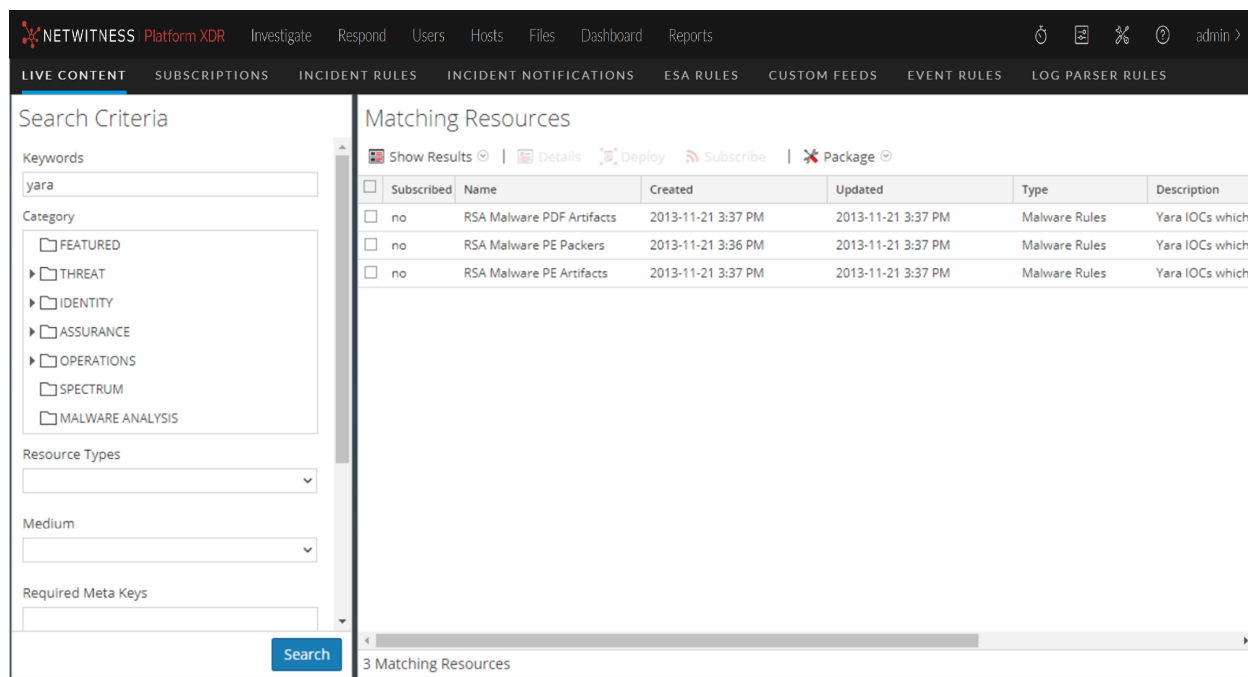
On the Malware Analysis host, the YARA rules reside in `/var/lib/netwitness/malware-analytics-server/spectrum/yara`, as shown in the example below.

```
[root@TESTHOST yara]# pwd
 /var/lib/netwitness/malware-analytics-server/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_packers.yara
```

The individual rules are listed as IOCs in the Malware Analysis Service Config view > Indicators of Compromise tab. To view them, use the Yara module as the filter. You can adjust the configuration of an individual in the same way that you configure other IOCs.

Add Custom YARA Rules

To introduce custom YARA rules from other sources:

1. To ensure that the YARA rules follows the correct format and syntax, use the YARA command to compile the YARA rule as shown in the following example. If the rule compiles with no errors, this indicates that the YARA rule has the correct syntax.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
   [root@TESTHOST yara]#
   ```

2. Ensure that custom rules do not duplicate existing YARA rules from other sources. All YARA rules are in `/var/lib/netwitness/malware-analytics-server/spectrum/yara`

3. Ensure that the meta keys supports are included to organize the YARA rules as part of the configurable IOCs, and name the file with the yara extension (<filename>.yara). For better organization, make sure that the `iocName` meta is included in the meta section as shown in the following example.

   Example:
   ```
   rule HEX_EXAMPLE
   ```

```
{
    meta:
        author = "RSA"
        info = "HEX Detection"
      iocName = "Hex Example"
    strings:
        $hex1 = { E2 34 A1 C8 23 FB }
        $wide_string = "Ausov" wide ascii
    condition:
        $hex1 or $wide_string
}
```

4. When ready, place the custom YARA file in the folder that the Malware Analysis service watches:

   `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`

   The file is consumed within one minute.

   Once consumed, NetWitness moves the file to the `processed` folder, and the new rule is added to the Malware Analysis Services Config view > Indicators of Compromise tab.

> **Note:** If you fail in adding the custom YARA rule, after step 4, do the following:
> 1. Check the custom YARA file is in `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch/error`.
> 2. Check the logs `/var/lib/netwitness/malware-analytics-server/spectrum/logs/spectrum.log`.

Examine Scan Files and Events in List Form

When viewing the Summary of Events in a Malware Analysis scan, you can click a file count or an event count to view the Files List or the Events List for the scan (see Begin a Malware Analysis Investigation). In the Files List and Events List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files. When you find an event or file of interest in the Events List or Files List, you can view many details about the event in the Event Details view.

For each event in the Events List, NetWitness provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.
- Antivirus vendor scores.
- The Influenced by customized rule flag.
- The date the event was archived.
- The session time.
- The MD5 hash filter.
- The number of files in the event.
- The source IP address of the event.
- The Identity.
- The destination IP address.
- The destination country.
- The name of the alias host.
- The event type, for example, Network.
- The service used by the event.
- The destination organization

For each file in the Files List, NetWitness provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.
- Antivirus vendor scores.
- The filename.
- The file type.
- The MD5 hash filter.
- The source IP address of the event that contained the file.

- The destination IP address.

- The date the event that contained the file was archived.

- The file size.

Sort the Files List or Events List

You can sort the Files List and Events List by column name in ascending and descending order. You can choose one or two columns.
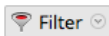
To sort the list:

1. In the first **Sort By** drop-down list, choose a column name and sort direction: for descending

   order or for ascending order.

2. (Optional) In the second **Sort By** drop-down list, choose a column name, and sort direction, for

   descending order or for ascending order.
   The column titles reflect the selected sort order.

Filter the List by Filename or MD5 File Hash

You can filter the Files List and Events List by filename or file hash. With this feature, you can specify a limited subset of the original data based on the search criteria.

> **Note:** When you perform a search, you search the scan that you are currently displaying, not all scans.

1. Click ▼ Filter ⊙ .
   The Filter dialog is displayed.

2. Enter a value in **File Name** or **MD5 Hash** and click **Filter**. The File Name and Hash field are not case sensitive. Wild card or regular expressions are not supported. The filter is based on exact matches. You can drag across a filename or hash to select from the Files list or Events list, then copy and paste it in the dialog.

3. Click **Filter**.
    Malware Analysis filters the list to display only files or events with the selected hash

4. To revert to the unfiltered list, click ▼ Filter ⊙ . When the Filter dialog is displayed, click **Reset**.

Download Files from the Files List

NetWitness lets you select and download files from the Files List or the Events List.

> **Caution:** Use caution when downloading files from Malware Analysis; some files may contain harmful code. File Download is a specific permission that can be configured, refer to "Define Roles and Permissions for Malware Analysts" in the *Malware Analysis Configuration Guide* for more details.

To download files from the Files List or Events List:

1. In the **Files List** or **Events List**, select the checkbox next to one or more rows.

2. In the toolbar, select ![Download Files] .
    The Malware File Download dialog is displayed.

3. Do one of the following:

    a. If you decide not to download the file, click **Cancel**.

    b. If you want to download the file, select click the **Download** button.
        The file or files selected are downloaded in a zip archive with the name `Malware_Files.zip`.

Delete Events from the Scan

In the Events List, you select one or more events and delete them from the scan. This is useful for removing events that are not of interest.

To remove an event from the scan being viewed:

1. In the **Events List**, select one or more events.

2. In the toolbar, click ![Delete Events] .
    NetWitness asks for confirmation that you want to delete the events.

3. In the confirmation dialog, click **Yes**.
    The selected events are deleted.

Return to the Summary of Events

To leave the Files List or Events List and return to the Summary of Events, click **Back to Summary**.

Open the Detailed Analysis for an Event

While you examine events or files in the Files List or Events List, you can double-click any event or file to open a detailed analysis of the event in the Events List or the event with which the file in the Files List is associated (see View Detailed Malware Analysis of an Event).

Configure the Malware Analysis Summary of Events View

The Summary of Events provides a summary of the scan being investigated, and below the summary are configurable dashlets such as visualization charts and listings. By default, the Summary of Events for a scan opens with the default dashlets displayed. You can customize the view by adding, modifying, and deleting default dashlets. The configured customization of dashlets persists through different scan investigations, and you can restore default dashlets at any time. The default dashlets are:

- Summary of Events (Fixed)

- Event Timeline

- Top Listing of Highly Suspicious Malware

- Meta Treemap

- Score Wheel

- Meta Breakdowns

The following figure is an example of the default Summary of Events.
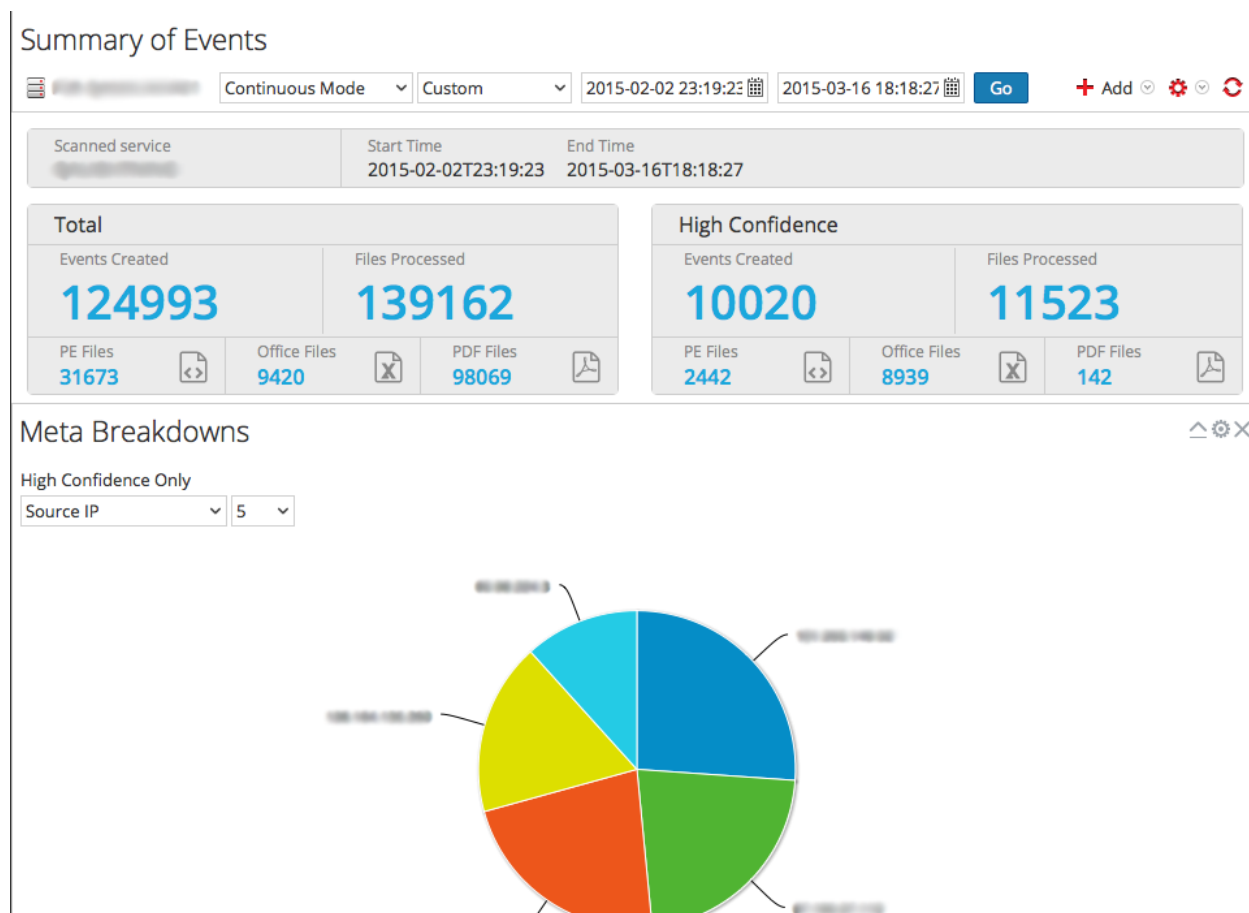
The rest of this topic provides instructions for managing and configuring dashlets.

Add a Dashlet

You can add multiple copies of dashlets in the Malware Analysis Summary of Events. To add a dashlet:

1. In the toolbar, select **Add**.
   The drop-down list of dashlets is displayed. There are four visualization options: Score Wheel, Meta Treemap, Meta Breakdowns, and Event Timeline. The other three dashlets are the same dashlets available in the NetWitness dashboard: Malware with high Confidence IOCs and High Scores, Top Listing of Highly Suspicious Malware, Top Listing of Possible Zero Day Malware. Details for these common dashlets are provided in "Dashlets" in NetWitness Content.

2. Select a dashlet.
   The new dashlet is added as the last dashlet below the existing dashlets.

3. If the dashlet is a duplicate of an existing dashlet, change the name of the new dashlet so that it is unique.

Modify or Delete a Dashlet Using Toolbar Options

Each dashlet has a toolbar that offers options for modifying the dashlet. The visualization charts have the same configuration settings, while some of the other dashlets have different additional settings.

Event Timeline	⌃⚙✕

To use the toolbar options:

- To close a dashlet so that only the title bar is displayed, click ⌃.

- To open a dashlet that is closed, click ⌄.

- To display the configurable settings for a dashlet, click ⚙.
  The settings dialog for the dashlet is displayed.

- To delete a dashlet, click ✕.

Apply Threshold Filter to Multiple Dashlets

Within dashlets, you can set a threshold to show only events equal to, above, or below a certain score in the four categories (Static, Network, Community, and Sandbox). This procedure sets the thresholds by dashlet type for these dashlets: Event Timeline, Score Wheel, and Meta Treemap. You can also set the threshold for individual dashlets.

1. In the toolbar, select ⚙ ⌄ > **Apply Threshold Filter**.
   The Apply Threshold Filter dialog is displayed.
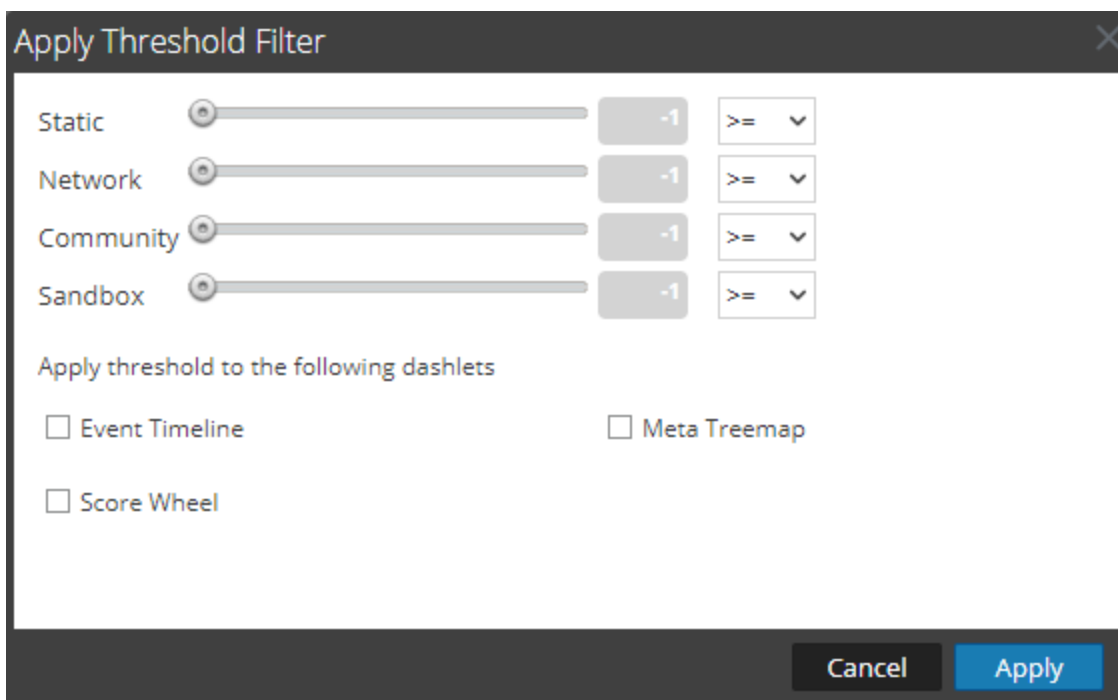
2. Select one or more dashlet types: Event Timeline, Score Wheel, and Meta Treemap.

3. Drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.

4. Click **Apply**.

   The threshold filters are applied to the selected dashlet types in the Summary of Events.

Set Title and Category Options for a Dashlet

1. To display the configurable settings for a dashlet, click ⚙.

   The Options dialog for the dashlet is displayed.
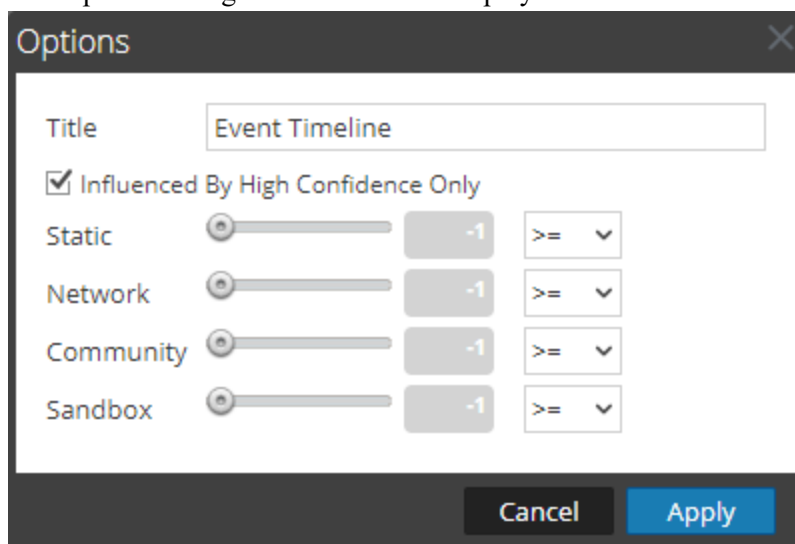
2. Type a new title for the dashlet in the **Title** field.

3. If you want to see only events that are influenced by a High Confidence tag, which means there is high confidence that the event contains harmful code, check the **Influenced By High Confidence Only** option.

4. If you want to see only events that were given a score above a certain score in the four categories (Static, Network, Community, and Sandbox), drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.

5. Click **Apply**.
   The title and filters are applied to the dashlet.

Order Dashlets

To change the order of dashlets as they appear beneath the Summary of Events:

1. In the toolbar, select ⚙ ⊙ > **Order Dashlets**.
   The Order Dashlets dialog is displayed.

   ![Order Dashlets dialog showing numbered list: 1 Event Timeline, 2 Top Listing of Highly Suspicious Malware, 3 Meta Treemap, 4 Score Wheel, with Up and Down buttons and Cancel/Apply buttons]
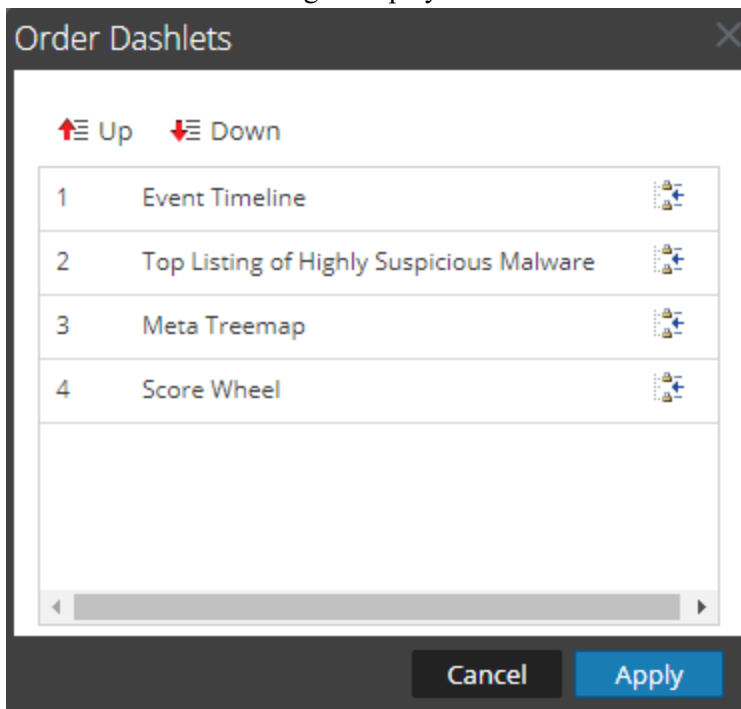
2. Select a dashlet that you want to move up or down, and click ⬆ Up or ⬇ Down.

3. When you are satisfied with the order, click **Apply**.
   The dialog closes and the order of dashlets below the Summary of Events is changed to match your choices.

Restore Default Dashlets

After you have added, modified, and arranged dashlets, you can revert to the default settings for dashlet display. To restore the default dashlets:

1. In the toolbar, select ✿ ⌄ > **Restore Default Configuration**.

   A dialog requests confirmation that you want to restore the configuration.

2. Do one of the following:

   a. If you decide to keep the dashlet arrangement you have configured, click **No**.

   b. If you are sure that you want to restore the defaults, click **Yes**,
      The dashlet display reverts to the default display.

Filter Dashlet Data in the Summary of Events View

The Summary of Events provides a summary of the scan being investigated with selectable dashlets. The Summary of Events is fixed, but Analysts can configure each dashlet to filter out information and drill into the data.

The rest of this topic provides instructions for managing and configuring dashlets.

Configure the Score Wheel Dashlet

The Score Wheel is a high-level visualization of analyzed sessions that scored high, medium, or low in each of the scoring categories: Static, Network, Community, and Sandbox. The Score Wheel is a quick way to drill into sessions to review them. Each ring represents a different scoring category so that you can visually compare results by category.

You can change the order of the rings to highlight indicators of compromise that were flagged in one category but not in another category. Comparing the same results in a different sequence of the rings provides visibility into additional vulnerabilities in a session, and you can drill into sessions of interest. The following examples show two possible use cases.

Zero-Day Candidates Example

This example shows how to drill into sessions that the Community did not flag as malicious, but all other scoring categories did. The resulting list of sessions highlights zero-day candidates.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)

2. Click the red slice in the outermost (Sandbox) ring that aligns with a green slice on the innermost ring (Community): green (innermost) -> **Static**: red -> **Network**: red -> **Sandbox**: red (outermost).
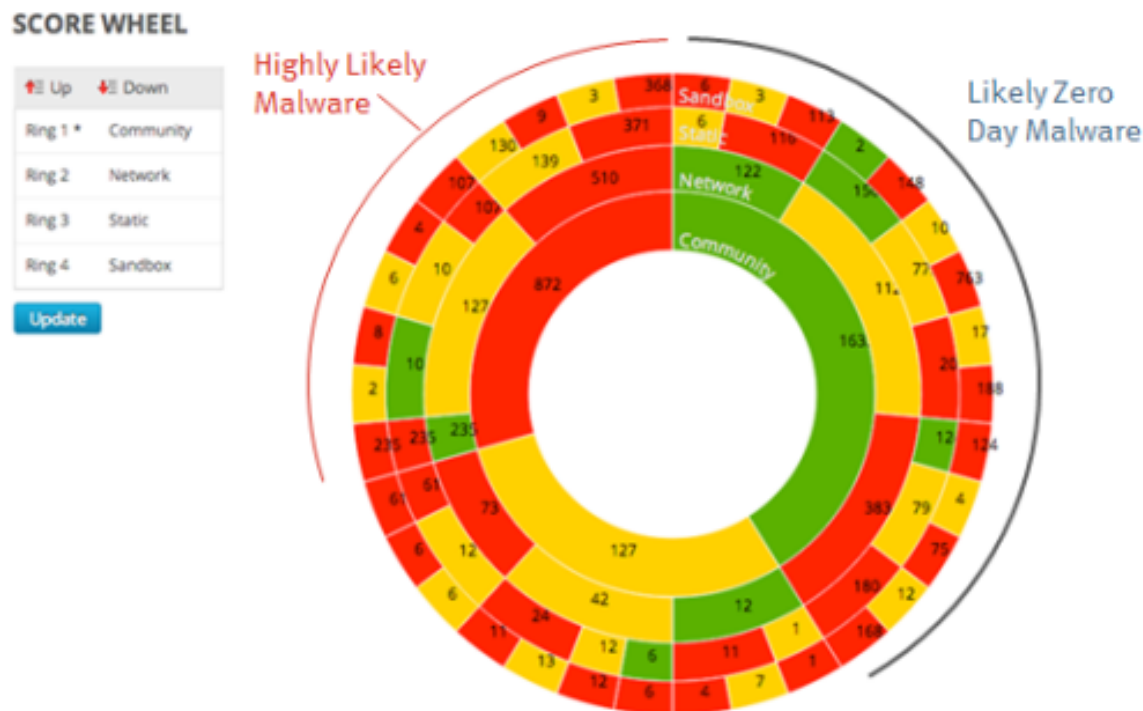
Malicious Sessions Example

This example shows how to drill into sessions in which all scoring categories identify the resulting list of sessions as malicious, indicating Malware Analysis has the most confidence that they are malware.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)

2. Click the red slice of the outermost (Sandbox) ring that aligns within a red slice on the innermost ring (Community): red (innermost) -> Static: red -> Network: red -> Sandbox: red (outermost).

Arrange the Ring Sequence by Scoring Module

In the Score Wheel, you can arrange the sequence of the rings by scoring module. Initially, the sequence of rings from inside to outside is Static, Network, Community, and Sandbox.

To change the ring sequence:

1. Do one of the following:

   a. Click and drag each scoring module up or down.

   b. Select each scoring module and use the Up and Down buttons to move it.

2. When the ring sequence is the way you want it, click the **Update** button.
   The Score Wheel is refreshed with the new sequence.
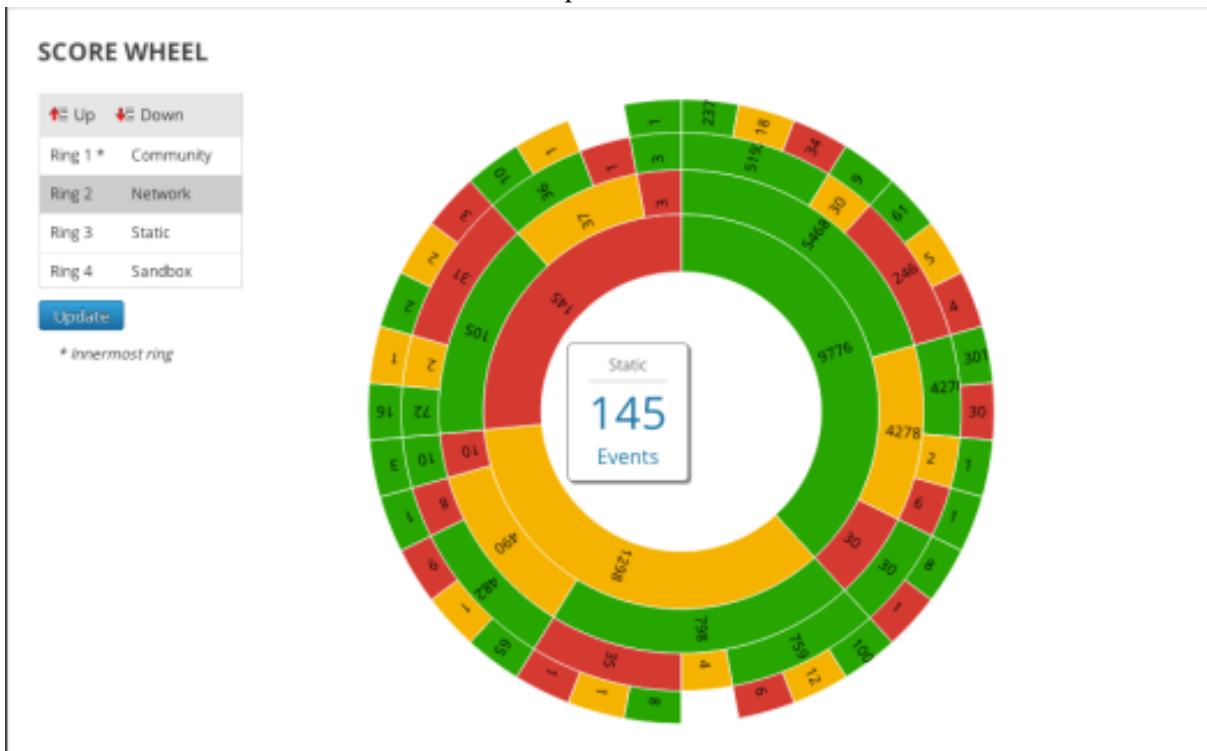
Configure the Meta Treemap Dashlet

In the Meta Treemap chart, you can visualize and filter meta breakdowns by meta type, count, and analysis type. Use the three selection lists to set the filter, and the Meta Treemap chart is refreshed immediately.
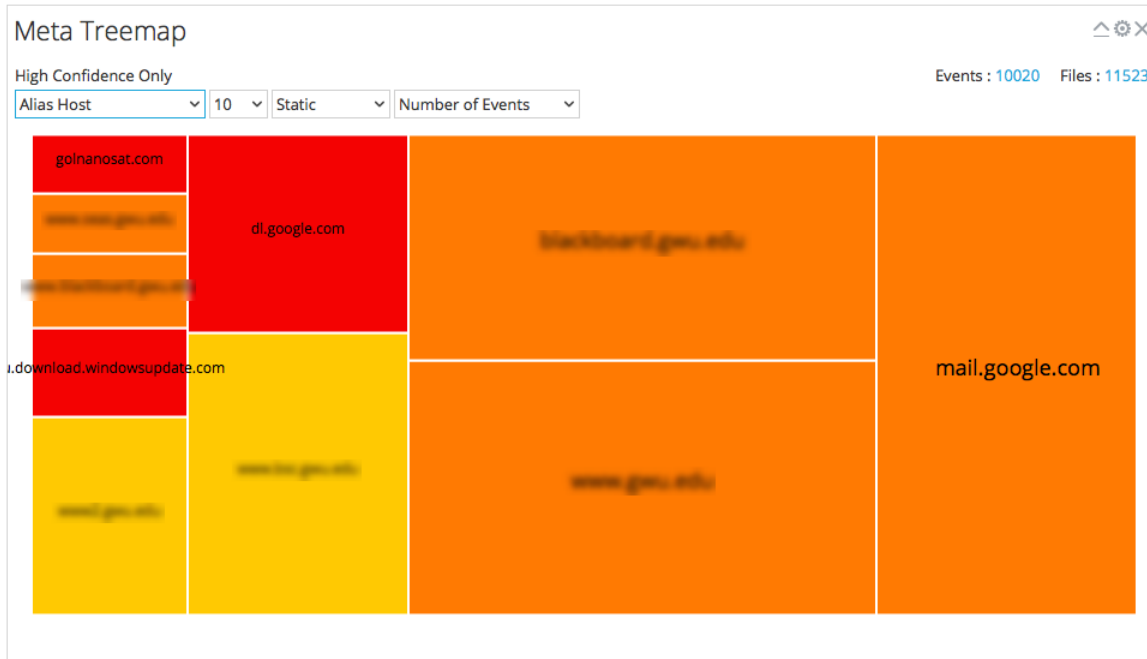
Configure the Meta Breakdowns Dashlet

The Meta Breakdowns dashlet is a visualization of values for a specific meta key in a pie chart. In the Meta Breakdowns chart, you can filter meta breakdowns by meta type and count. Use the two selection lists to set the filter, and the Meta Breakdowns chart is refreshed immediately.
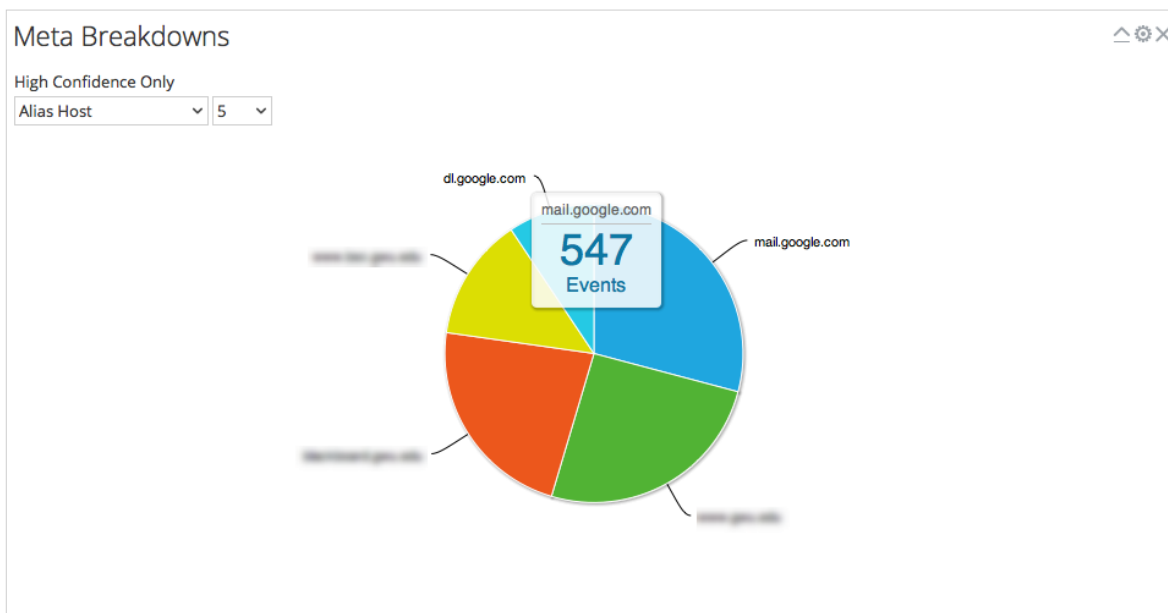
Configure the Events Timeline Dashlet

The Events Timeline dashlet is a visualization of the events along a timeline. No additional filters are available for the Event Timeline.
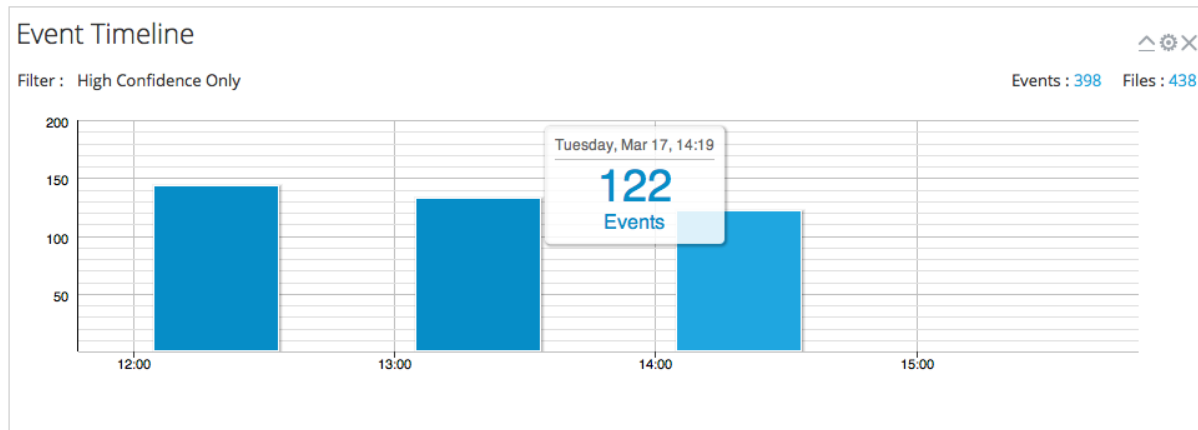
Open All Events in the Events List

From within the Event Timeline, you can open the entire list of events in the Events List. To do so, click
View Events . This option is not the same as clicking the count next to Events, which is the same for all visualization charts and opens the current drill point in the Events List.

Configure the Top Listing of Highly Suspicious Malware Dashlet

The Top Listing of Highly Suspicious Malware Dashlet presents the Top 10 most suspicious events in the Events List or the Files List. This dashlet is also available in the Monitor dashboard, and the configuration options are described as part of the NetWitness Content in Dashlets.
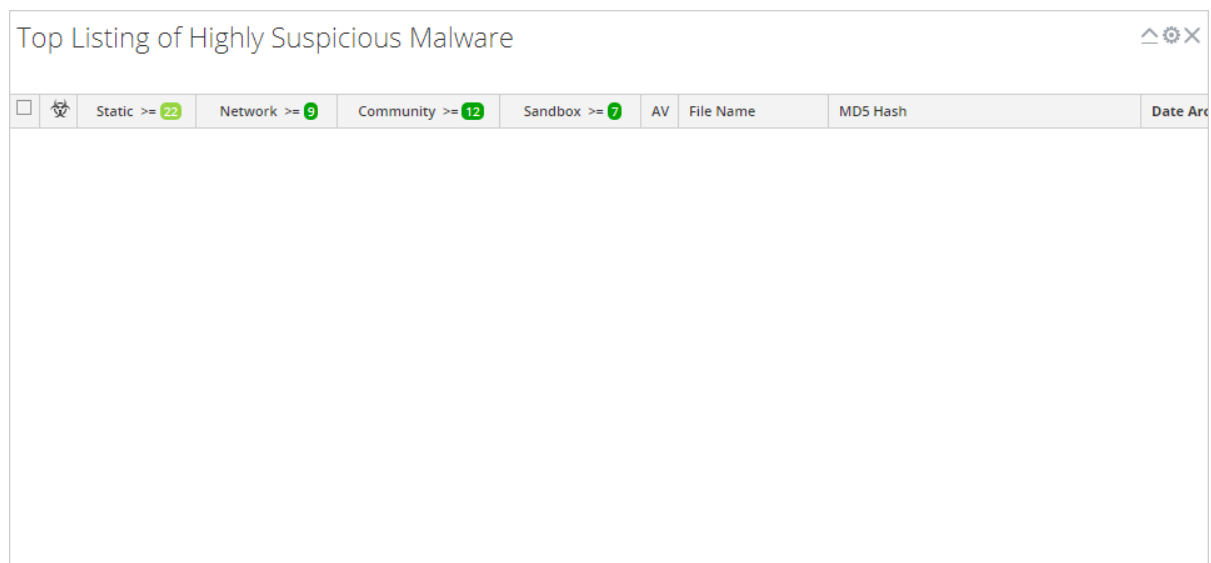
Configure the Malware with High Confidence IOCs and High Scores Dashlet

The Malware with High Confidence IOCs and High Scores dashlet presents Indicators of Compromise that have both high scores and high confidence that the events are likely to contain malware. The dashlet is also available in the Unified dashboard, and the configuration options are described as part of the NetWitness Content in Dashlets.
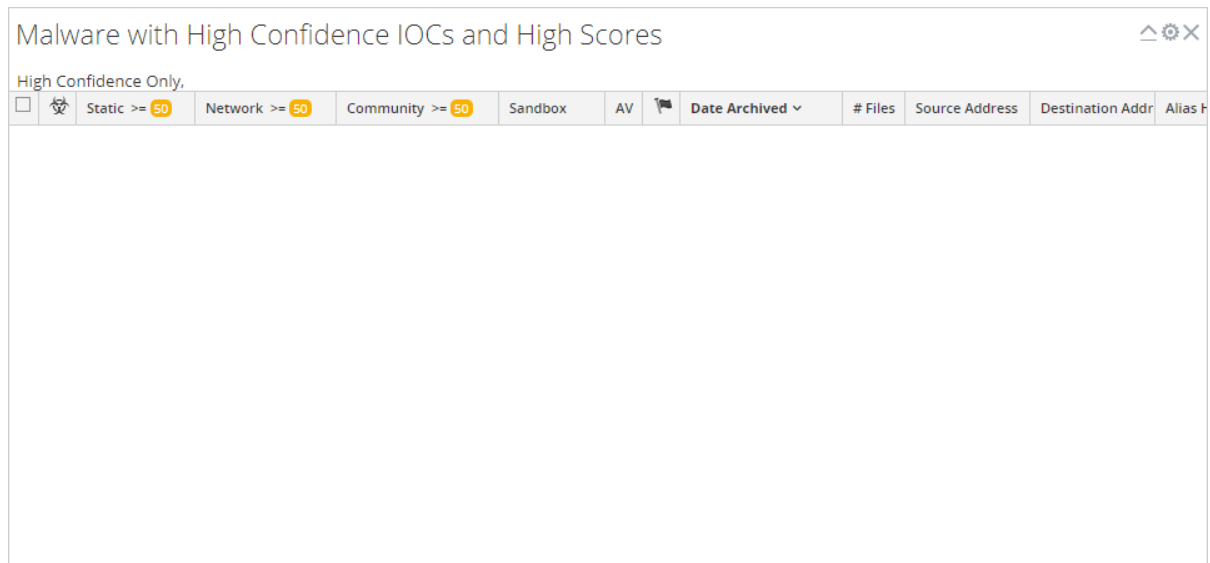
Configure the Top Listing of Possible Zero Day Malware Dashlet

The Top Listing of Possible Zero Day Malware dashlet presents potential zero day events in the Events List or the Files List. The dashlet is also available in the Unified dashboard, and the configuration options are described as part of the NetWitness Content in Dashlets.

		Static >= 80	Network >= 80	Community <= 0	Sandbox	AV		Date Archived	# Files	Source Address	Destination Addr	Alias Host
☐	☣	100	98	0				2015-05-07T12:37:...	1	- protected -	- protected -	- protected -
☐	☣	81	100	0				2015-05-07T12:31:...	1	- protected -	- protected -	- protected -
☐		100	100	0				2015-05-07T12:24:...	2	- protected -	- protected -	- protected -
☐		81	87	0				2015-05-06T21:34:...	1	- protected -	- protected -	- protected -
☐		81	87	0				2015-05-06T21:34:...	1	- protected -	- protected -	- protected -
☐		100	87	0				2015-05-06T21:34:...	1	- protected -	- protected -	- protected -
☐		100	87	0				2015-05-06T20:21:...	1	- protected -	- protected -	- protected -
☐		100	87	0				2015-05-06T20:21:...	1	- protected -	- protected -	- protected -

Top Listing of Possible Zero Day Malware

Time = Last 5 Days,

Upload Files for Malware Analysis Scanning

There are two methods for analysts to upload files for Malware Analysis scanning.

A Malware Analyst with permission to Initiate Malware Analysis Scan can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog.

It is also possible to upload a file for scanning using a watched file share.

Upload Files Manually

This topic provides instructions for initiating on-demand scanning of an uploaded file. When you upload a file for scanning, NetWitness starts the upload job and adds it to the jobs queue. When the job is complete, you can view the scan in Malware Analysis.

To upload a file to scan:

1. Go to **Investigate > Malware Analysis**.

   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel.
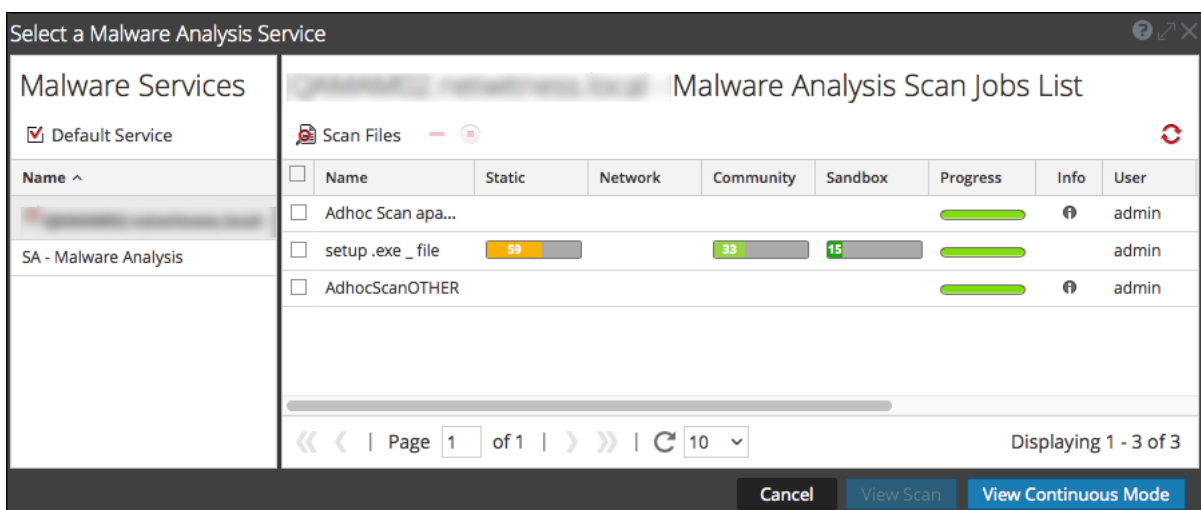
2. Click **View Scan**.

   The Scan for Malware dialog is displayed.
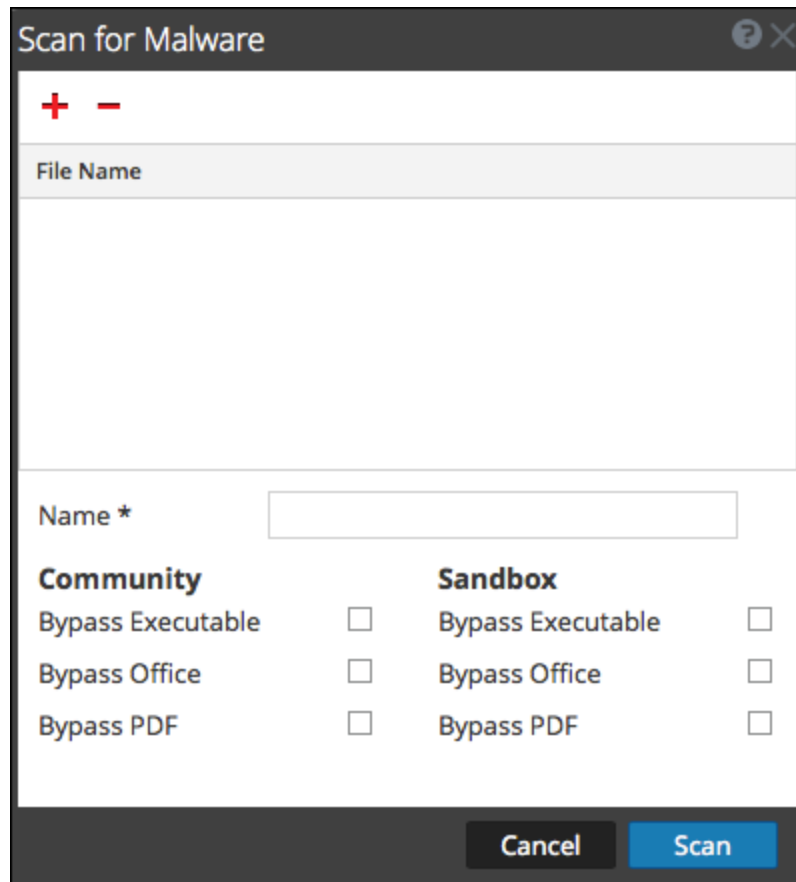
3. Click **+**

A view of the files system is displayed so that you can choose files to upload.

4. Select one or more files from the list and click **Open**.

The file names are added. Malware Analysis escapes the filename characters before processing a file. The maximum number of filename characters after escaping is 200. If the filename is greater than 200 characters, Malware Analysis truncates the filename characters and displays the truncated filename in the NetWitness user interface.

5. Continue adding and deleting files until you have a list of the files that you want to upload.

6. Name the scan and select the types of files to bypass. This is useful for a zip archive that contains different types of files, and overrides the default bypass settings.

7. Click **Scan**.

The scan job is submitted and NetWitness displays a confirmation message for successful submission. The scan request is added to the Scan Jobs List dashlet. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.

8. The job is added to the Scan Jobs List in the Select a Malware Analysis Service dialog and in the Unified dashboard Scan Jobs List dashlet.

9. To view the scan when complete, double-click the scan.

The Malware Summary of Events for the selected scan is displayed.

Upload Files from a Watched Folder

To upload files from a watched folder, you can drop files into a watched file share for Malware Analysis. Analysts can share YARA rules, hash files, and infected zip archives with Malware Analysis.

Malware Analysis watches a file share and automatically consumes files placed in specific folders in the file share. This feature is useful for:

- Bulk import of hash files from `/var/lib/rsamalware/spectrum/hashWatch`.

- Addition of custom-YARA rules to the Indicators of Compromise (IOC) list on the host from `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`.

- Creation of on-demand scan jobs from a zip archive of infected zip files from `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Analysts need to prepare the files for consumption in accordance with requirements, the file extension must be correct, and the file must be copied to the correct watched folder in the file share.

Import a Hash List

To import a hash list from the watched directory, the hash list must be in the specified format and must be sorted on md5. You can drop a file formatted into a folder (`/var/lib/rsamalware/spectrum/hashWatch`) on the Malware Analysis host, and it is automatically imported into the local hash database. This is described in "Configure Hash Filter" in the *Malware Analysis Configuration Guide.*

To import a hash list using the watched folder method:

1. Copy the hash lists that you want to import into the **/var/lib/rsamalware/spectrum/hashWatch** directory.
   NetWitness Malware Analysis automatically watches this folder and processes files placed there.

   a. Malware Analysis adds every hash found in the hash lists to the hash filter.

   b. If there are processing errors, they are logged in:
      `/var/lib/rsamalware/spectrum/hashWatch/error`

   c. Processed files are cataloged
      here: `/var/lib/rsamalware/spectrum/hashWatch/processed`

   d. Processed files are not removed from the hashWatch directory.

2. After importing hashes in bulk, the System Administrator can use a cronjob to clean up old processed files.

Import YARA rules to the IOC List

Customers with advanced skills and knowledge can add detection capabilities to Malware Analysis by authoring YARA rules and publishing them in Live or placing YARA rules in a watched folder for the host to consume. Implement Custom YARA Content provides complete information on the prerequisites for using custom YARA content and authoring rules.

When the rules are ready, place the custom YARA files in the folder that the Malware Analysis service watches:
`/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
The file is consumed within one minute.
Once consumed, NetWitness moves the file to the `processed` folder, and the new rule is added to the Malware Analysis Service Config view > Indicators of Compromise tab.

Import Files into the Scan Jobs List

When you obtain samples from perimeter security solutions and would like to perform further analysis on the files, you can zip the files and password protect the archive with `infected`, then add to the watched folder for consumption by Malware Analysis. This zipped archive is ready to be placed in the watched folder: `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

> **Note:** The maximum size of the archive is 100 MB.

To analyze infected, password-protected zip files, Malware Analysis consumes archives place in a watched folder and creates an on-demand job that is added to the Scan Jobs List.

1. While logged on as administrator, place the files to be processed in a zip file with password `infected` at `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   In a minute or two Malware Analysis consumes the archive and creates an on-demand job in the Scan Jobs List. The scan job name is the name of the file, the user is **file share**, and the Event Type is 1. The archive is moved to
   `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`

2. After the job is added to the Scan Job List, run a script or cronjob to clean up the zip file in `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

View Detailed Malware Analysis of an Event

When viewing the list of individual events in a Malware Analysis scan in the Malware Analysis Events grid, you can double-click an event to view the detailed analysis results for the event.

View Malware Analysis Details for an Event

1. Start an investigation in the **Malware Analysis** view.
   The Malware Summary of Events is displayed, and includes four charts, including the Event Timeline.

2. Do one of the following:

   a. To view all events in the Event Timeline, click the **View Events** button.

   b. Double-click data in the **Meta Breakdown**, **Meta Treemap Chart**, or **Score Wheel**.
      The Events List is displayed.

3. Double-click an event.
   The Analysis Results for the event are displayed.
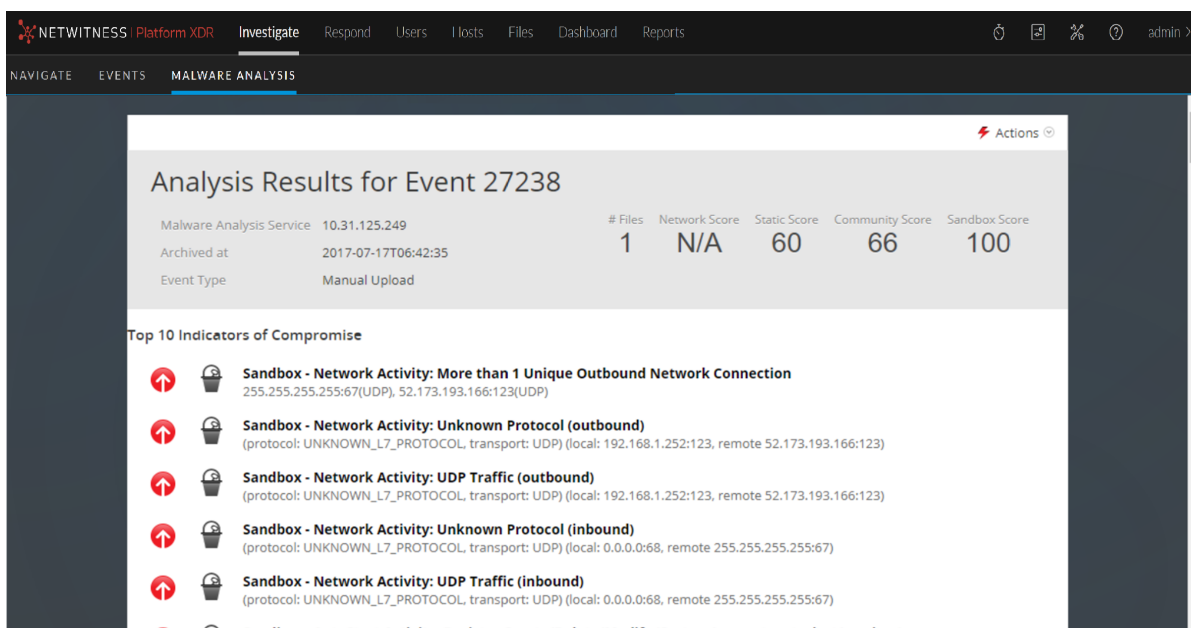
4. (Optional) If you want to delete an event, select **Actions > Delete Event**.

5. If you want to view a reconstruction of the network session, select **Actions > View Network Session**.
   The session opens in the Navigate view > Event Reconstruction.

Pivot Network Analysis Results

You can pivot the Network Analysis Results in several ways:

1. Scroll down to the Network Analysis Results.

2. Hover over a meta value and left-click.
   The context menu is displayed.
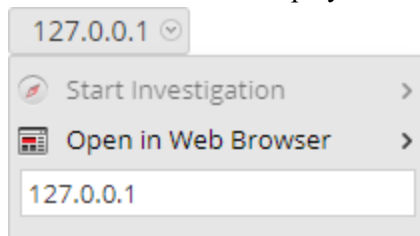
3. To view the selected meta value in the **Navigate** view, select **Start Investigation** and a time option.

4. To view the selected meta value in a browser, select **Open in Web Browser > Open in Google**.
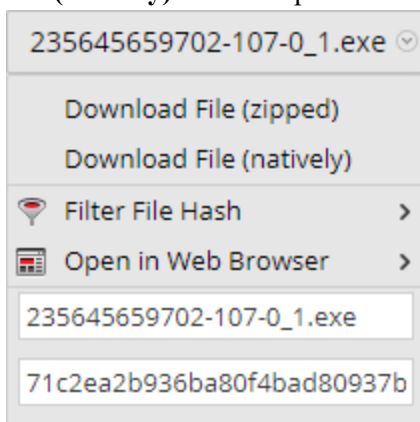
Use File Actions in the Static Analysis Results

1. Scroll down to the Static Analysis Results.

2. If you want to download a file, select the file name and either **Download File (zipped)** or **Download File (natively)** in the drop-down menu. It is safer to download a file in zipped format.

3. If you want to mark the file as safe or unsafe in the hash list, select **Filter File Hash** and **Mark hash as good** or **Mark hash as bad**.

View Community Analysis Results Details

The Community Analysis Results summarizes results from the community, identifying Indicators of Compromise that were flagged as a risk or identified as good.

In addition, this view lists the results from Installed AV Vendors and Not Installed AV Vendors. You can compare results of the installed AV vendors that were configured for the current Malware Analysis service versus Community results. You can also see results from a list of AV vendors that are not configured as installed for the current Malware Analysis service.

Each row of AV vendor results includes the shield icon to show whether the IOC was discovered by a Primary (🛡) or Secondary AV (🛡) vendor in the community, the name of the Installed or Not Installed vendor, and the name of malware or risk detected by the community and AV vendor. If the AV vendor did not detect a risk, **-- Not detected --** is displayed instead of the name of the risk.

The Not Installed AV Vendors section is expandable to view all entries, but is collapsed by default to minimize the need to scroll. Clicking the + expands the list.

If no installed AV vendors have been configured for the current Malware Analysis service, the following message is displayed: No AV vendors were marked as installed. Please go to the Malware Analysis Service configuration page to identify installed AV vendors.
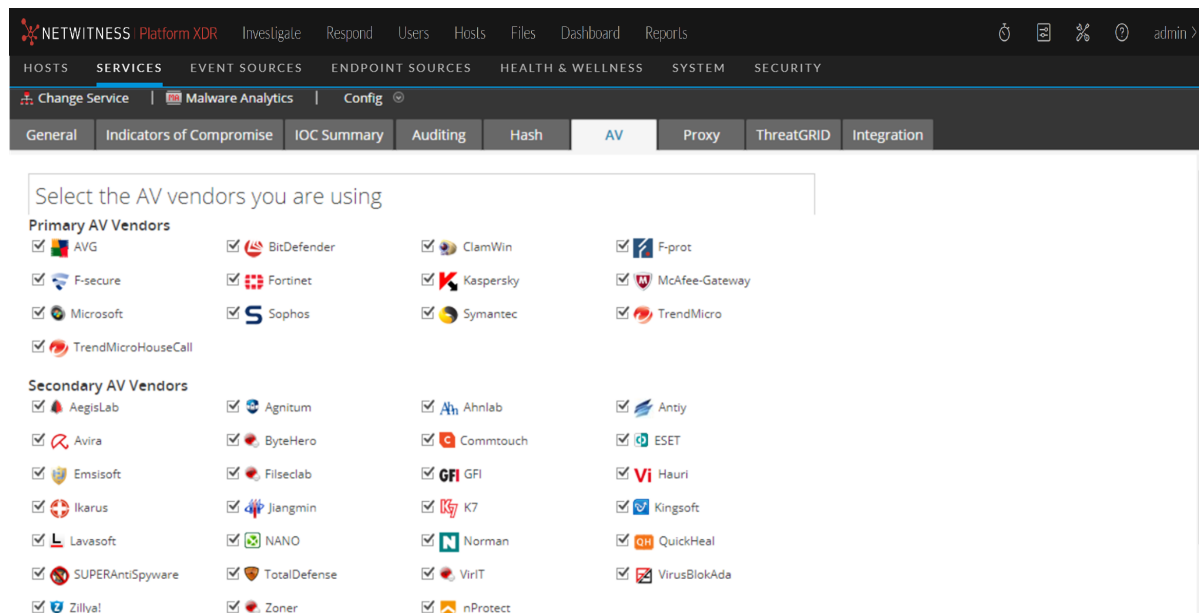
View Sandbox Analysis Results in the ThreatGRID User Interface

If you have registered with ThreatGRID, you can view the Sandbox results directly in ThreatGRID.

1. Scroll down to the Sandbox Analysis Results.

100   **Sandbox Analysis Results**

Number Files Downloaded 0	Number Outgoing Sockets 0
Number Processes Spawned 16	Number Sockets with Unknown Protocol 8
Number Incoming Sockets 0	Process Runtime 0
Number of Sockets Listening 0	Process Status N/A
Vendor Name ThreatGrid	Analysis Id 52bba6514d37b1760d78a44b082b735f
Number of UDP Sockets 9	Number of Registry Modifications 1
Number of Firewalled Connections 0	Number of File Modifications 9

2. Click the **Analysis ID** and select **Open In ThreatGRID**.
   The analysis report in ThreatGRID is displayed.

Malware Analysis Reference Materials

This section provides is intended to help you understand the purpose and application of Malware Analysis views in NetWitness Investigate. For each view, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition some of the reference materials include workflows and Quick Looks to highlight important features in the user interface.
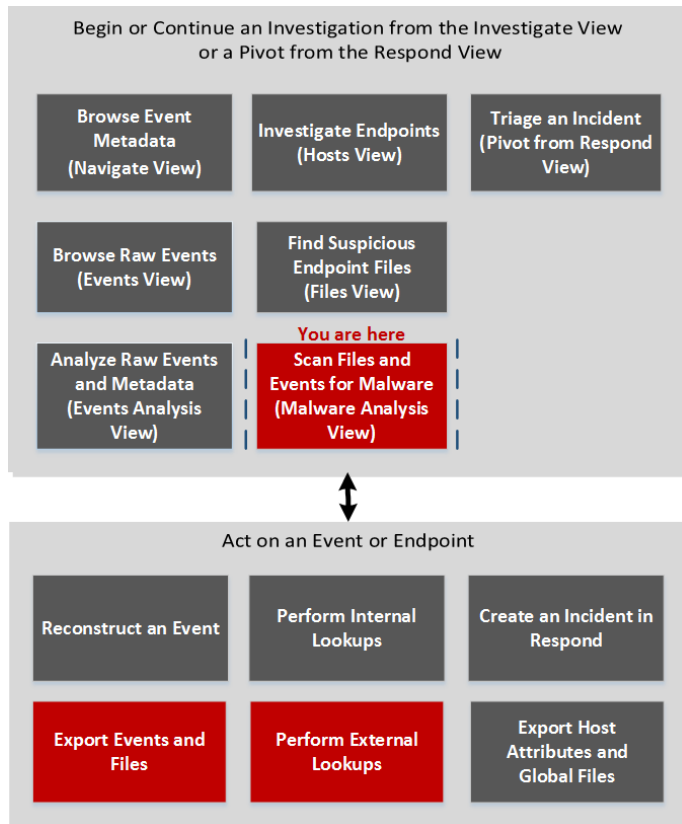
- Malware Analysis View
- Malware Analysis Events List and Files List
- Scan For Malware Dialog
- Select a Malware Analysis Service Dialog

Malware Analysis View

In NetWitness Investigate, the Malware Analysis view provides the user interface for conducting a malware analysis. The Malware Analysis view is in the form of a customizable dashboard, in which default dashlets in the initial view are based on the user role (Administration or Analyst) and user customizations. Initially, the Summary of Events dashlet is displayed in the Malware Analysis view. Additional dashlets present different visualizations of the events being viewed, and each representation is configurable to further refine your view as you search for Indicators of Compromise. The Malware Analysis dashlets available in the Dashboard are also available in the Malware view.

To access this view, select **Investigate > Malware Analysis**. If a default service has not been selected, the Select a Malware Analysis Service dialog is displayed. Select a service, then click **View Continuous Mode**.

Workflow

What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	browse event metadata	*NetWitness Investigate User Guide*

User Role	I want to ...	Show me how
Threat Hunter	browse raw events	*NetWitness Investigate User Guide*
Threat Hunter	analyze raw events and metadata	*NetWitness Investigate User Guide*
Threat Hunter	investigate endpoints (Version 11.1)	*NetWitness Investigate User Guide*
Threat Hunter	find suspicious endpoint files (Version 11.1)	*NetWitness Investigate User Guide*
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Investigate User Guide*
Threat Hunter	export events and Files*	Examine Scan Files and Events in List Form
Threat Hunter	perform external lookups*	View Detailed Malware Analysis of an Event

*You can perform this task in the current view.

Related Topics

- "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*
- "Launch a Malware Analysis Scan from the Navigate View" in the *NetWitness Investigate User Guide*

Quick Look

Below is an example of the Malware Analysis view.

The Malware Analysis view consists of the Summary of Events panel and four dashlets unique to this view. Each of the unique dashlets have identical Options dialogs. The Malware Analysis dashlets in the MONITOR view are also available, and are described in the Dashlets topic in the NetWitness Content space.

Summary of Events Panel

In the Summary of Events panel, you can select the service, the scan mode, and the time range. In addition, you can select a data point and view the events associated with the event.

The following table describes all features in the Summary of Events panel.

Feature	Description
	Selects a service to display.
Scan Mode	Displays a drop-down list of available scan modes.
Time Range	Displays a drop-down list of time ranges to view events.
Start Date	When Time Range is set to custom, offers a calendar from which to choose the start date of the time range.

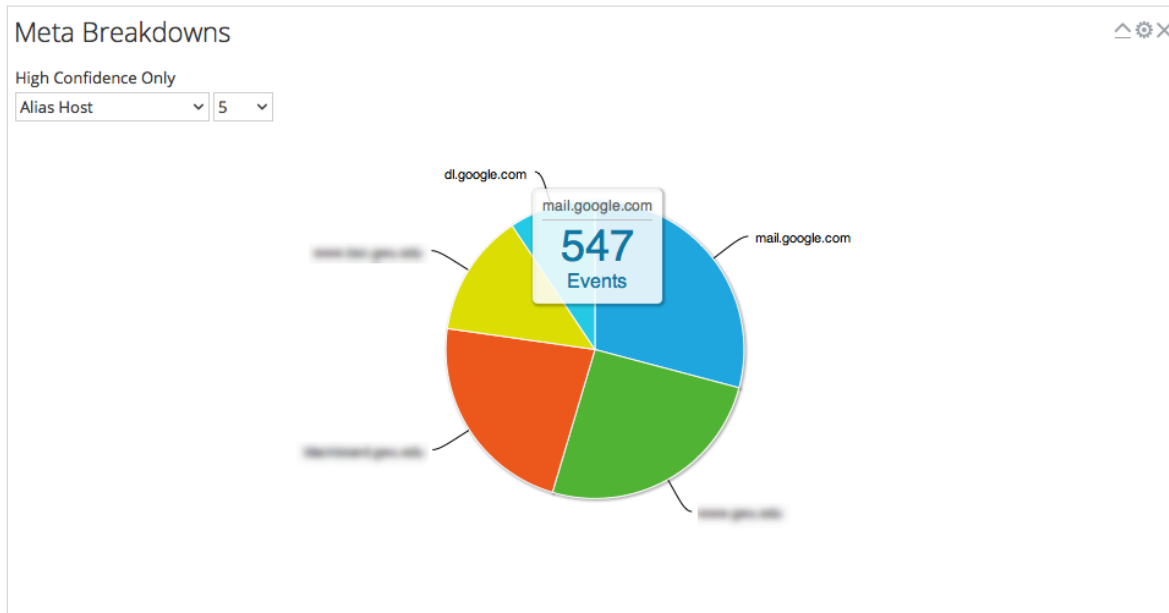| Feature	Description
End Date	When Time Range is set to custom, offers a calendar from which to choose the end date of the time range.
✚ ⌄	Displays a drop-down list of dashlets you can add to the view.
✿ ⌄	Displays a drop-down list of actions you can perform in this view: • Restore Default Configuration • Order Dashlets • Apply Threshold Filter
⟳	Refreshes the Malware Analysis view.

Options Dialog

In the Options dialog, you can customize the results displayed in the dashlet. This dialog can be accessed by clicking the ✿ icon in the top right corner of each dashlet. The following table describes the features of the Options dialog.

Feature	Description
Title	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Influenced By High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence.
Static, Network, Community, Sandbox	Allows you to filter results based on the scores in the scoring modules.
Cancel	Closes the dialog without saving any changes.
Apply	Applies changes to the dashlet immediately and closes the dialog.

Meta Breakdowns

Meta Breakdowns presents events in the form of a pie chart, with each slice representing a meta value for the specified meta key. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta value having the most events. Hovering over an event displays the count.

The following table describes the options in the Meta Breakdowns dashlet.

Feature	Description
High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Meta Key	Drop-down list of available meta keys.
Count	Drop-down list specifying how many of the top results are displayed.

Meta Treemap

Meta Treemap presents events in the form of a heat map. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta values having the most events. In addition, you can select the module that detected the meta value in the events: static, network community, or sandbox.

The following table describes the options in the Meta Treemap dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
Meta Key	Drop-down list of available meta keys to select as a filter.
Count	Drop-down list specifying how many of the top results are displayed.
Module	Drop-down list specifying which module results will be pulled from.
Value	Drop-down list specifying what information will be displayed when the mouse is hovering over a result (for example, Average Score).

Score Wheel

The Score Wheel offers a view of events as concentric rings with colors representing scores for events based on Indicators of Compromise and the scoring module. You can arrange the position of the rings using the Up and Down arrows to obtain a view that highlights events that were detected by one scoring module (red) and not detected by other scoring modules.

The following table describes the features of the Score Wheel dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
Module Order grid	Displays the order of the rings in Score Wheel, Ring 1 being the innermost ring and Ring 4 being the outermost ring. You can click the **Up** and **Down** buttons to reorder the modules, then click **Update** to apply the changes.

Event Timeline

The Event Timeline offers a view of events organized by the time of occurrence in a bar graph. Clicking and dragging to select a time range within the chart zooms in on the selected time.
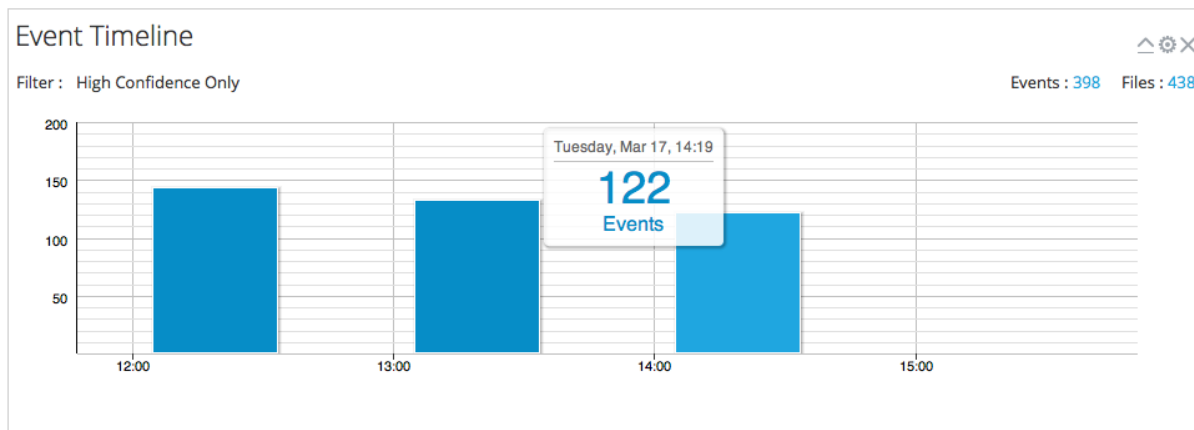
The following table describes the features of the Event Timeline dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
View Events	Displays the Investigate > Events view.

Malware Analysis Events List and Files List

The Malware Analysis Events List and Files List provide a detailed view of events or files. You can double-click on an event or file in either of the lists to display the Analysis Results view in a new browser tab.

To access this view, go to **Investigate > Malware Analysis** > **Select a Malware Analysis Service** dialog. Select a service from the left panel, then select a job from the right panel, and click **View Scan**. In the Summary of Events view do one of the following:

- In either the **Total** panel or the **High Confidence** panel, click the number in the **Events Created** section.

- If you want to view the Files List, click the number in the **Files Processed** section.

Workflow

What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	browse event metadata	*NetWitness Investigate User Guide*

User Role	I want to ...	Show me how
Threat Hunter	browse raw events	*NetWitness Investigate User Guide*
Threat Hunter	analyze raw events and metadata	*NetWitness Investigate User Guide*
Threat Hunter	investigate endpoints (Version 11.1)	*NetWitness Endpoint User Guide*
Threat Hunter	find suspicious endpoint files (Version 11.1)	*NetWitness Endpoint User Guide*
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	export events and Files*	Examine Scan Files and Events in List Form
Threat Hunter	perform external lookups*	View Detailed Malware Analysis of an Event

*You can perform this task in the current view.

Related Topics

- "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*

Quick Look

This is an example of the Events List view.

This is an example of the Files List view.

These are the features in the Events List toolbar, and the Files List toolbar is the same, except it has no option to delete events.
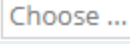
Feature	Description
Back to Summary	Returns to the Summary of Events view.
Delete Events	Removes the selected events from the current events list.
Download Files	Displays the Malware File Download dialog, which allows you to download available files.
Choose ...	Displays a drop-down menu from which you can decide how to sort the list. These are the options for sorting: • High Confidence • Static • Network • Community • Sandbox • AV • File Name • File Type • Hash • Date Archived • Size The button directly to the right of this drop-down indicates whether the list will be sorted by ascending or descending values.
Choose ...	Displays a drop-down menu from which you can select a secondary sorting order. This menu includes an option forNetWitness**None**, so selecting a secondary sorting order is not necessary.
Filter	Displays a drop-down window in which you can filter the list by filename or MD5 Hash.

These are the features in the Events List.

Feature	Description
☣	Indicates whether the event is influenced by the high confidence flag.
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.

Feature	Description
🏳	Indicates whether the event is influenced by a customized rule.
Date Archived	Displays the date and time the event was archived.
Session Time	Displays the time of the event's session.
⊞	Indicates whether the hash value is marked as trusted.
# Files	Displays the number of files included in the event.
Source Address	Displays the address of the event source.
Identity	Displays the identity of the event source.
Destination Address	Displays the address of the event destination.
Destination Country	Displays the country of the event destination.
Alias Host	Displays the hostname of the alias.
Event Type	Displays the type of event. For example, Manual Upload.
Service	Displays the service on which the event occurred.
Destination Organization	Displays the organization of the destination.

These are the features in the Files List grid.

Feature	Description
☣	Indicates whether the event is influenced by high confidence flag.
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.
File Name	Displays the name of the file.
File Type	Displays the type of the file (for example, PDF or x86 PE)
MD5 Hash	Displays the MD5 hash.
Source Address	Displays the address of the file source.
Destination Address	Displays the address of the file destination.
Date Archived	Displays the date and time the file was archived.
Size	Indicates the size of the file.

Scan For Malware Dialog

In the Scan for Malware dialog, Malware Analysis analysts can upload files to investigate in Malware Analysis.

To access this dialog go to the **Malware Analysis** view. In the **Select a Malware Analysis Service** dialog, select a service in the left panel, then click Scan Files in the right panel.

Workflow

What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	browse event metadata	*NetWitness Investigate User Guide*
Threat Hunter	browse raw events	*NetWitness Investigate User Guide*
Threat Hunter	analyze raw events and metadata	*NetWitness Investigate User Guide*

User Role	I want to ...	Show me how
Threat Hunter	investigate endpoints (Version 11.1)	*NetWitness Endpoint User Guide*
Threat Hunter	find suspicious endpoint files (Version 11.1)	*NetWitness Endpoint User Guide*
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

- "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*

- Begin a Malware Analysis Investigation

- "Launch a Malware Analysis Scan from the Navigate View" in the *NetWitness Investigate User Guide*

Quick Look

The figure below illustrates the Scan for Malware dialog, and The following table describes the features available in the dialog.
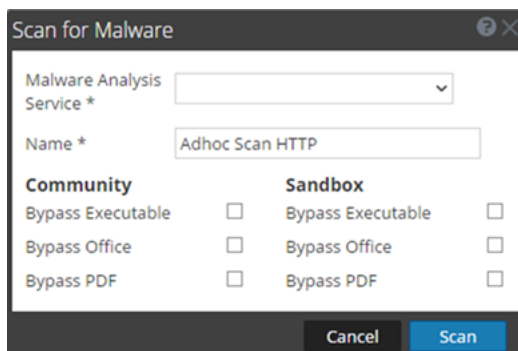
Feature	Description
✚	Uploads a file from your computer.
−	Deletes a file from the list.
File Name	Displays the names of the files added to the list.
Name	Allows you to name the scan job.

Feature	Description
Community	Displays options for Community to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Sandbox	Displays options for Sandbox to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Cancel	Closes the dialog without performing any actions.
Scan	Scans the uploaded files.

Select a Malware Analysis Service Dialog

The Select a Malware Analysis Service dialog is accessible in the Malware Analysis view. In this dialog, Malware Analysis analysts can select a service to investigate, choose a scan on that service to investigate, upload a file to scan, and begin a continuous scan of the service.

Workflow
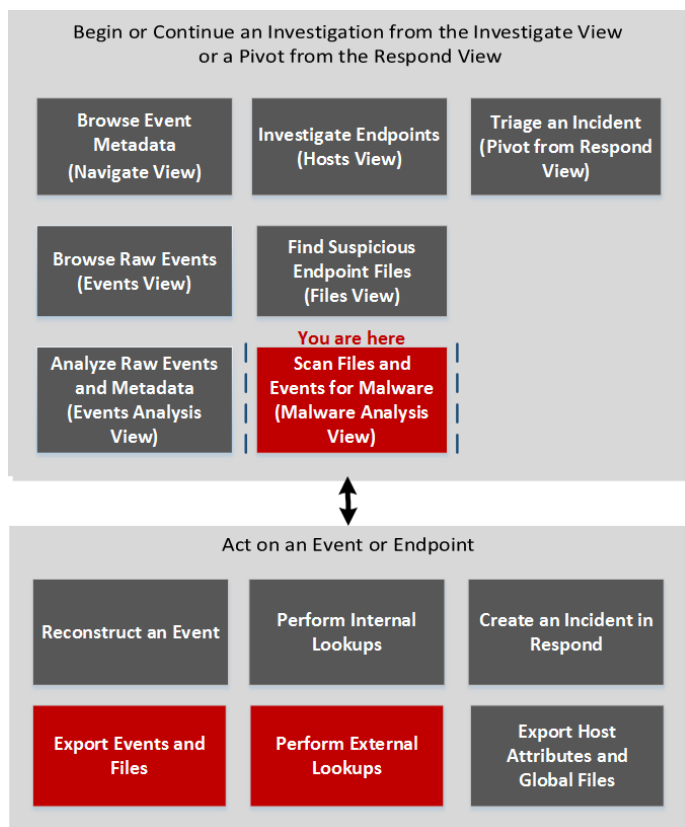
What do you want to do?

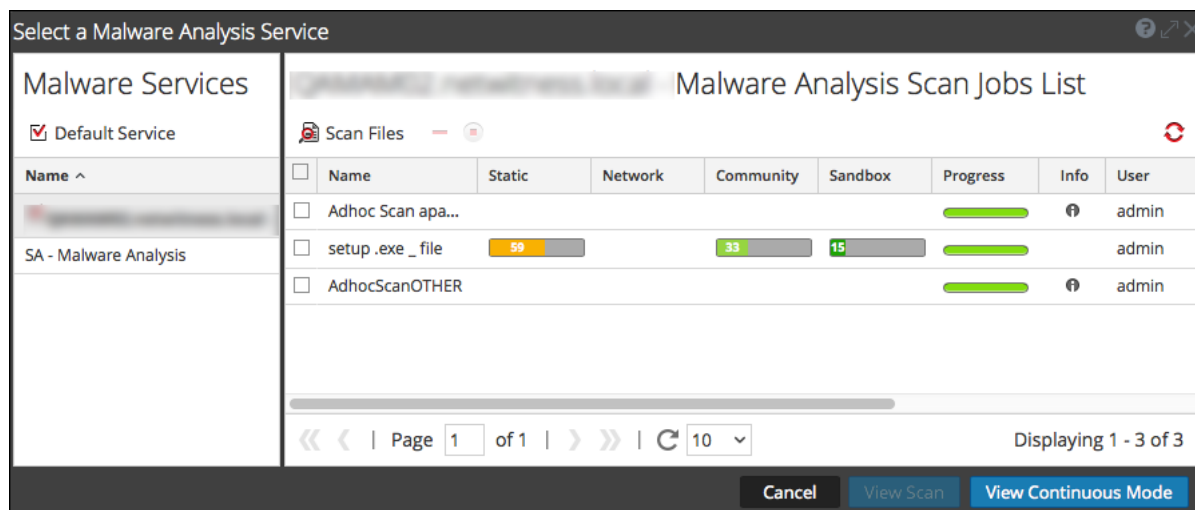| User Role	I want to ...	Show me how
Threat Hunter	browse event metadata	*NetWitness Investigate User Guide*
Threat Hunter	browse raw events	*NetWitness Investigate User Guide*
Threat Hunter	analyze raw events and metadata	*NetWitness Investigate User Guide*
Threat Hunter	investigate endpoints (Version 11.1)	*NetWitness Endpoint User Guide*

User Role	I want to ...	Show me how
Threat Hunter	find suspicious endpoint files (Version 11.1)	*NetWitness Endpoint User Guide*
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

- "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*

- Begin a Malware Analysis Investigation

- "Launch a Malware Analysis Scan from the Navigate View" in the *NetWitness Investigate User Guide*

Quick Look

The Select a Malware Analysis Service dialog has a Malware Services panel on the left and a Scan Jobs List on the right. The Scan Jobs List panel has a toolbar, list, and buttons to view scans.

The Malware Services panel is a list of services available for malware analysis. In this panel, you can select the service to investigate and you set a default service using the Default Service icon. When you select a service, the available scan jobs for that service are listed in the Scan Jobs list.

These are the features in the Scan Jobs List toolbar.

Feature	Description
Scan Files	Displays the Scan for Malware dialog, in which you can upload a file to the service for scanning.

Feature	Description
Delete scan job (➖)	Deletes one or more selected scan jobs, NetWitness displays a confirmation dialog before deleting scan jobs.
Cancel scan job (⏹)	Pauses or continues one or more scan jobs.
Refresh (🔄)	Refreshes the list of scan jobs.

These are the columns in the Scan Jobs list. This list is also available in the Malware Scan Jobs dashlet.

Feature	Description
Name	Displays the name of the job.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module.
Progress	Displays the current progress made on the job. • Green: The job is finished. • Black: The job is in progress. • Red: An error occurred.
Info	Provides additional information. Displays the query for the job. If the job is not complete, it also displays more detailed description of the status.
User	Displays the name of the user who created the job.
Events	Counts the number of events for the job.
Dropped	Counts the number of files or events in the job that were dropped because the scores are below their configured threshold.
Event Type	Displays the type of job: Manual Upload, On Demand, or Resubmit.
Scheduled	Displays the date and time when the job was executed.

These are the available actions in the dialog.

Feature	Description
Cancel button	Cancels the selected scan job.
View Scan button	Displays the Summary of Events for the selected scan with the default dashlets displayed.
View Continuous Mode button	Displays the Summary of Events for the selected scan with the default dashlets displayed.