NetWitness® Platform XDR

Version 12.0.0.0

Release Notes

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.

August, 2022

Contents

What's New

The NetWitness 12.0.0.0 release provides new features and enhancements for every role in the Security Operations Center.

Upgrade Paths

The following upgrade paths are supported for NetWitness 12.0.0.0

- NetWitness 11.6.0.0 to 12.0.0.0
- NetWitness 11.6.0.1 to 12.0.0.0
- NetWitness 11.6.1.0 to 12.0.0.0
- NetWitness 11.6.1.1 to 12.0.0.0
- NetWitness 11.6.1.2 to 12.0.0.0
- NetWitness 11.6.1.3 to 12.0.0.0
- NetWitness 11.6.1.4 to 12.0.0.0
- NetWitness 11.7.0.0 to 12.0.0.0
- NetWitness 11.7.0.1 to 12.0.0.0
- NetWitness 11.7.0.2 to 12.0.0.0
- NetWitness 11.7.1.0 to 12.0.0.0
- NetWitness 11.7.1.1 to 12.0.0.0

For more information on upgrading to 12.0.0.0, see Upgrade Guide for NetWitness 12.0.0.0

Security Fixes

For more information on Security Fixes, see Security Advisories.

Product Version Life Cycle for NetWitness Platform

See for Product Version Life Cycle for NetWitness Platform a list of versions that reach End of Primary Support (EOPS).

Enhancements

The following sections are a complete list and description of enhancements to specific capabilities:

- Policy Based Centralized Content Management
- Springboard
- Respond
- Investigation
- User Interface
- Endpoint Investigation
- Concentrator, Decoder, and Log Decoder Services
- Event Stream Analysis (ESA)
- Reports

To locate the documents that are referred to in this section, go to the NetWitness Master Table of Contents.

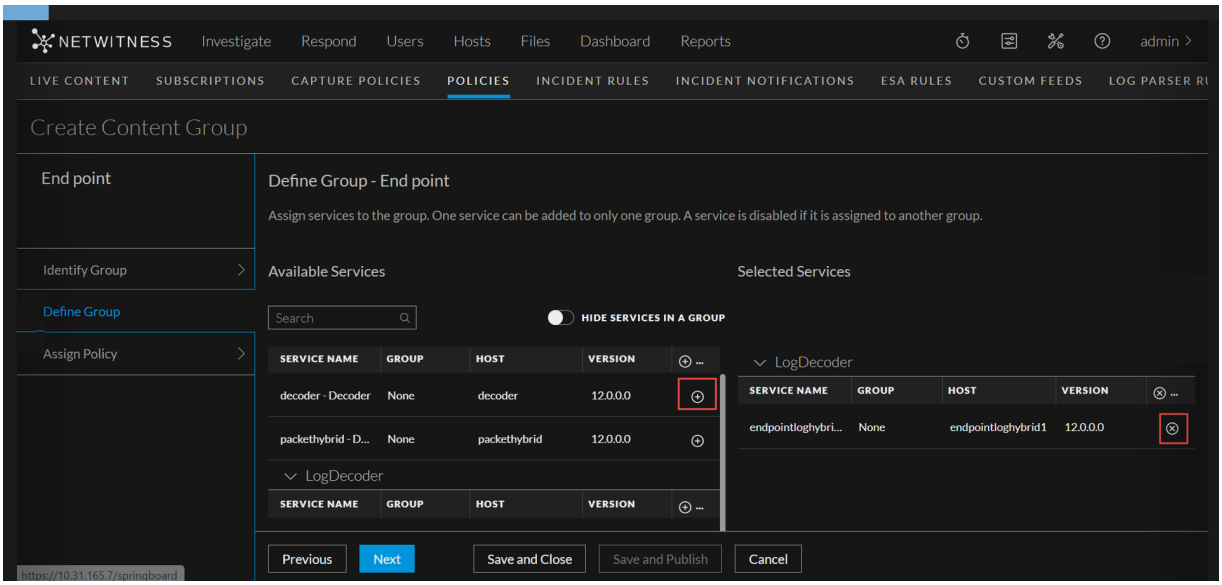
The Product Documentation section has links to the documentation for this release.

Policy Based Centralized Content Management

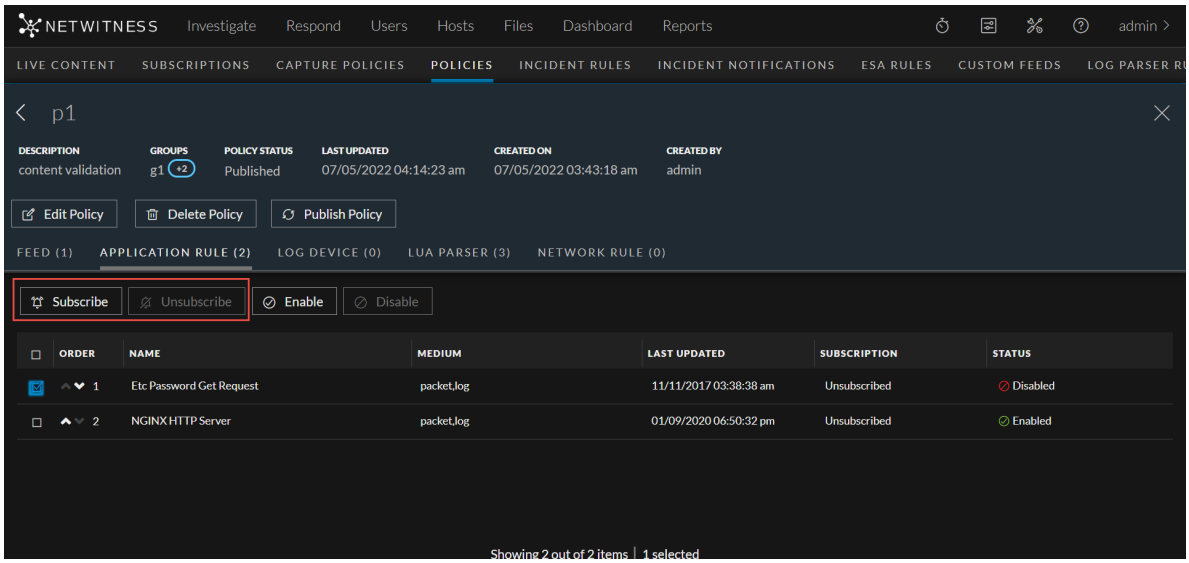
Policy based Centralized Content Management is a unified approach to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.

Benefits of Policy based Centralized Content Management:

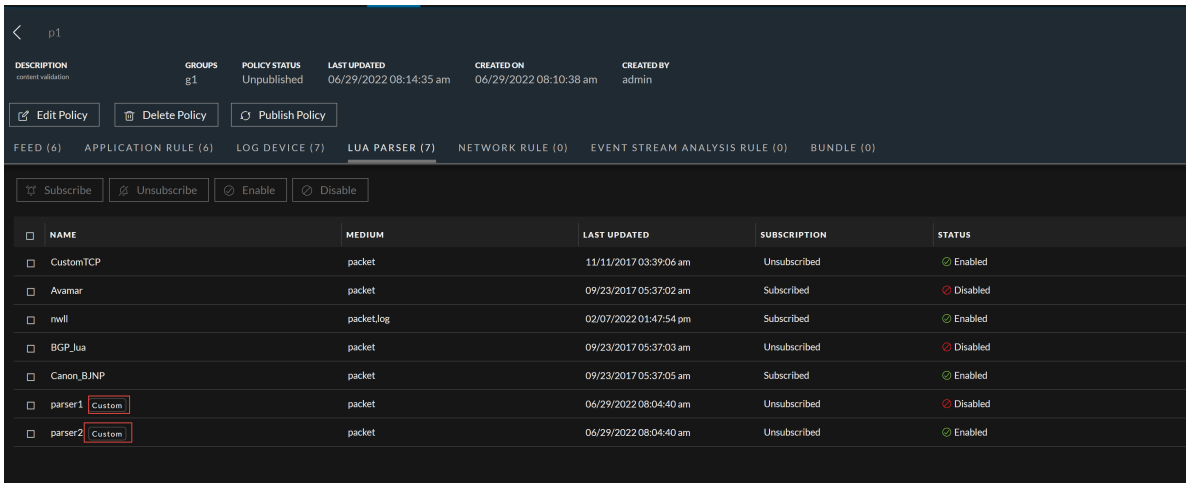
- Add content from RSA Live or add your own custom content.
- Add or remove content without repeating the process on each individual service.
- Add a new service to an existing group to automatically deploy all necessary content.



- One-click management of subscriptions and automatic updates
  - Simply toggle the **Subscribe** button to enable automatic updates of content.



- Provide highly responsive and updated UI for browsing RSA Live content that can help you with the following:
  - View Live and custom content along with your content policies and click  to add content.
  - Seamlessly view Live content along with your own custom content.
  - Centrally import and deploy live and custom content.



For more information, see *Policy based Centralized Content Management* topic in the Live Services Management Guide.

Springboard

The following section describes the new enhancements for the Springboard component:

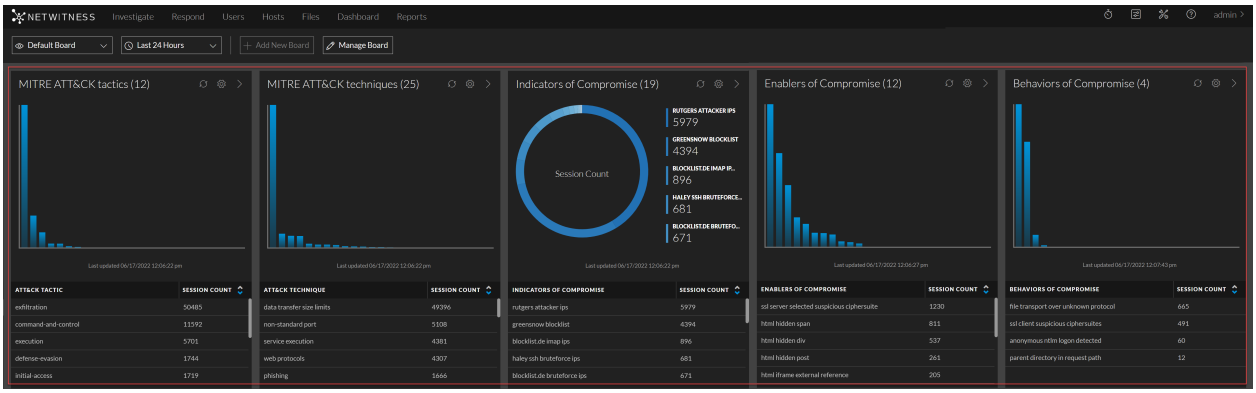
Enhanced Springboard to Support New Built-in Panels

NetWitness Platform Springboard introduces five more out-of-the-box panels based on the events processed and presented on Springboard view. On the Springboard, Administrators and Analysts can now view the following panels of events data which helps in threat hunting and investigation:

- **MITRE ATT&CK tactics**
- **MITRE ATT&CK techniques**
- **Indicators of Compromise**
- **Enablers of Compromise**
- **Behaviors of Compromise**

Administrators can customize these panels to display only the event-focused data for analysts to carry out further investigation.

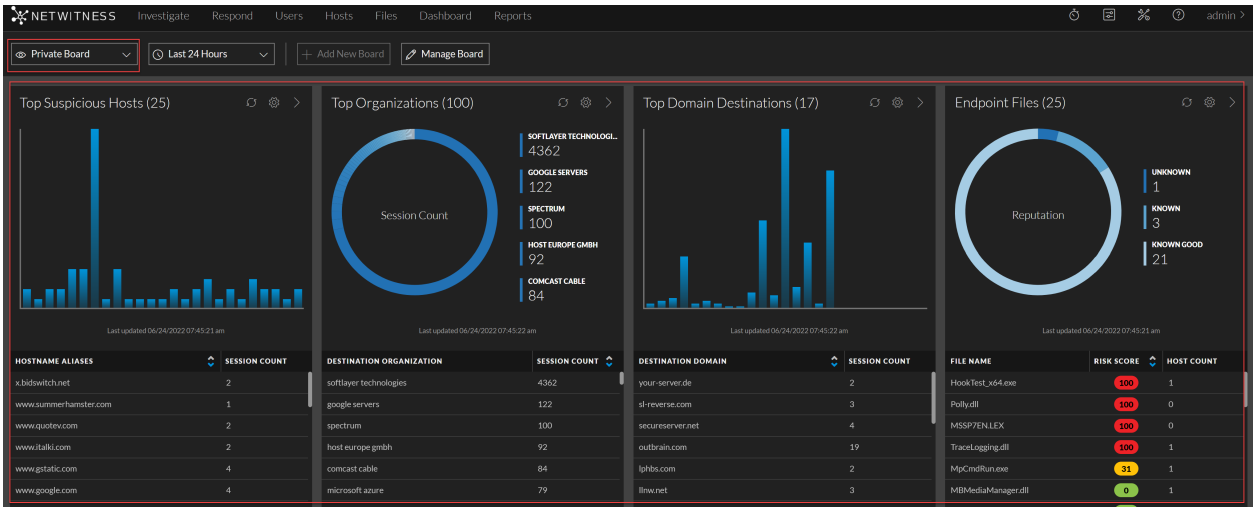
For more information, see *Managing the Springboard* topic in NetWitness Platform Getting Started Guide.



Create Custom Springboard at the User Level

Administrators and Analysts can now add their own custom private board to the NetWitness Platform Springboard and add panels with important system indicators, which helps in threat hunting and investigation. The custom private board is visible only for users who created it. The board allows users to organize and manage information in an easy manner.

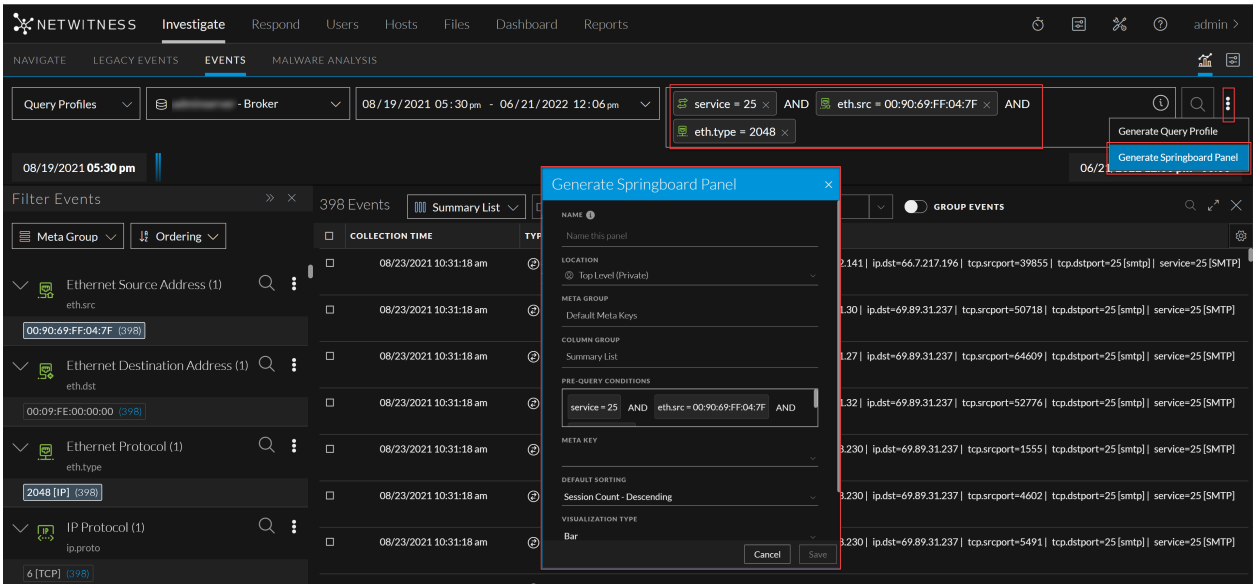
For more information, see *Managing the Springboard* topic in NetWitness Platform Getting Started Guide.



Automated Custom Springboard from Query

During investigation, Administrators and Analysts can add a Springboard panel from the **Investigate** > **Events** view. You can add any number of filters on the query search bar and convert them to Springboard panels for further detection and watch results. The newly added panels will be saved under a custom private board. The board will allow users to organize and manage information in an easy manner.

For more information, see *Add Springboard Panels from Events view* topic in NetWitness Platform Investigate User Guide.



Respond

The Respond view is enhanced to track and capture all the events performed by the users on an incident. The toolbar actions are enhanced to allow users select only the valid priority, status, and assignee for an incident.

Incident Workflow Enhancements

The following changes have been made to the **Change Status** drop-down list in the **Respond** > **Incidents** view:

- Added the new Incident status **Reopen** to help users open the closed incidents.
- Removed **New** and **Assigned** statuses but they are still displayed in the Status column in the **Respond** > **Incidents** > **Incidents List** view.
- Streamlined the incident status change workflow. All the invalid statuses are grayed out, allowing the users to select only the valid status for any incident.

  For more information, see *Escalate or Remediate the Incident* topic in the NetWitness Respond User Guide.

Incident Details View Enhancements

The new **History** Panel is added to display 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

  For more information, see *Incident Details View* topic in the NetWitness Respond User Guide.

Incident Overview Panel Enhancements

The Incident Overview Panel is enhanced to include the following fields:

- **Time to Acknowledge**(tta): Displays the time taken to assign an Incident after creating it.
- **Time to Detect**(ttd): Displays the time taken for completing the task after the Incident is assigned.
- **Time to Resolve**(ttr): Displays the time taken for closing the task after the Incident is created.
- **External ID**: Allows storing the Incident ID referrals from a different platform.

  For more information, see *Incident Overview Panel* topic in the NetWitness Respond User Guide.

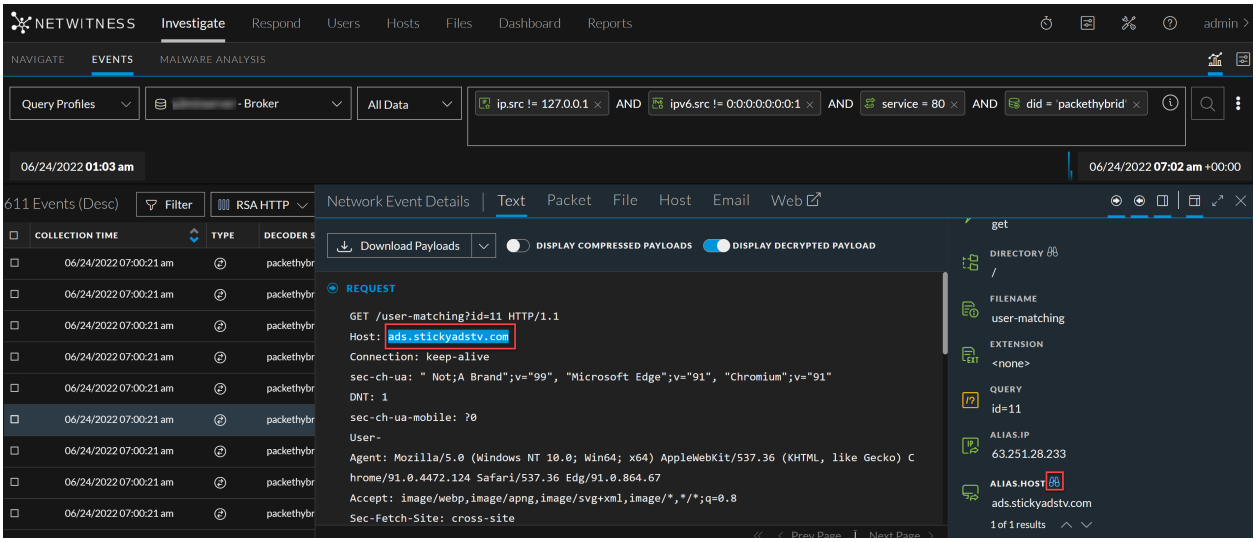
Investigation

The following section describes the new enhancements for the Investigation component:

Indicators for Searchable Meta

The meta key and meta value pairings now display a binocular icon while viewing a text reconstruction in the Event Meta panel, indicating the search option. This enhancement helps the analysts to visually see the indication rather than going through the list of all metadata to figure out which ones may be searched.

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

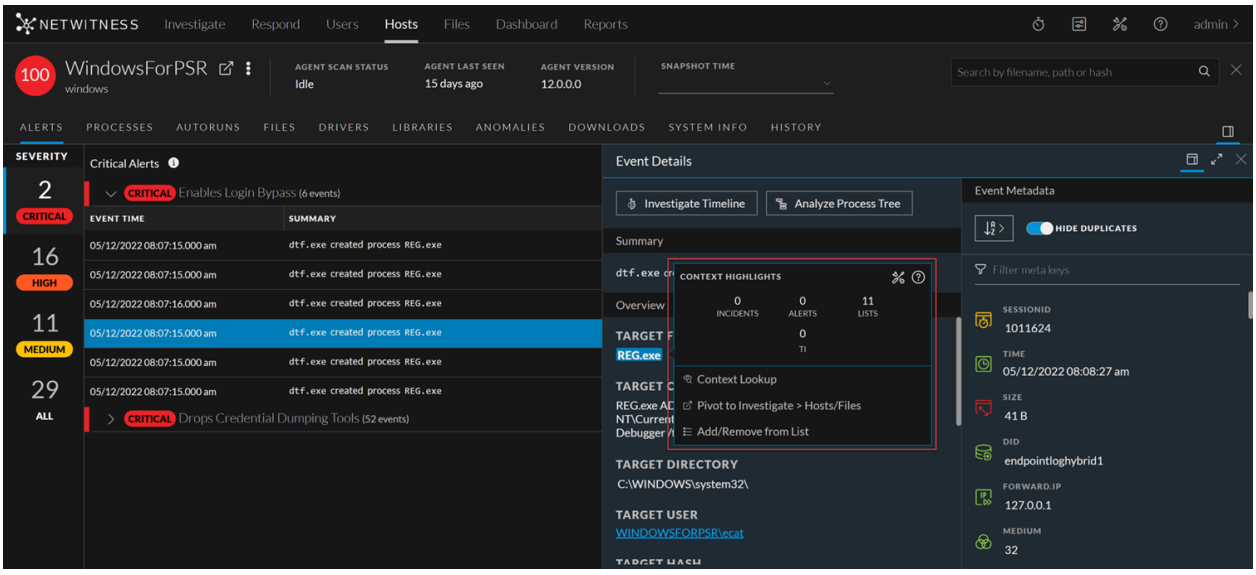


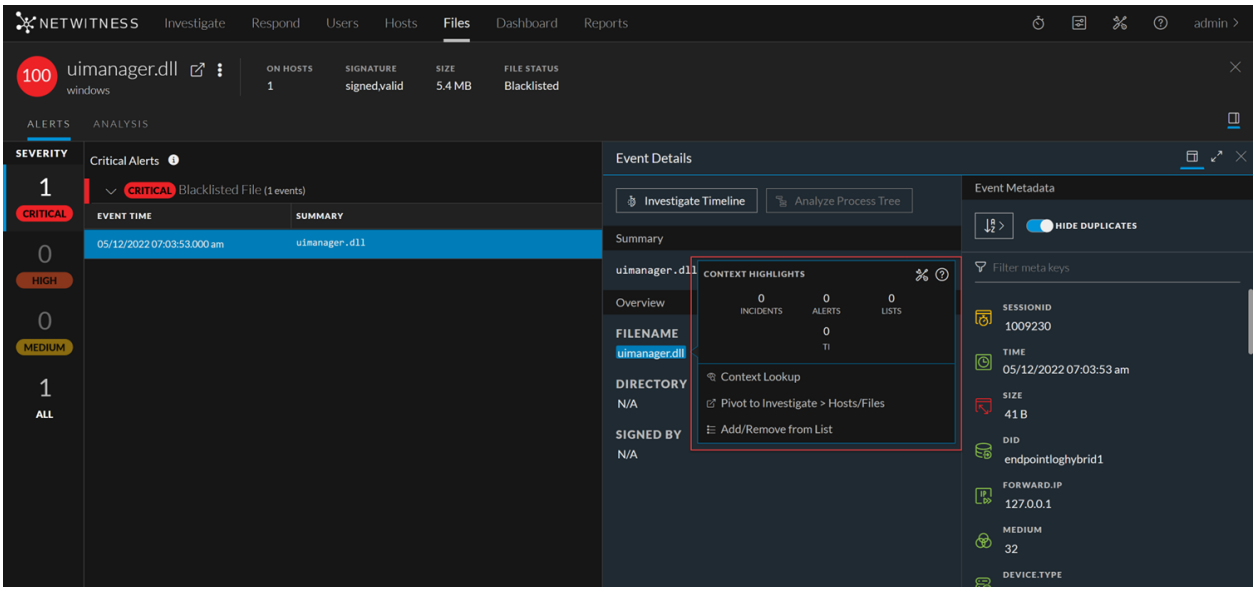
Unified Discovery and Interaction of Events Metadata

Hosts and Files Alerts Details View

Analysts have a unified way to interact with events metadata presented in the Alerts tab of Hosts and Files details view to perform actions or review contextual information. Analysts can use the right and left click options to view the unified panel data.

For more information on Hosts and Files, see *Analyze Hosts Using the Risk Score* and *Analyze Files Using the Risk Score* topics in NetWitness Platform Endpoint User Guide.

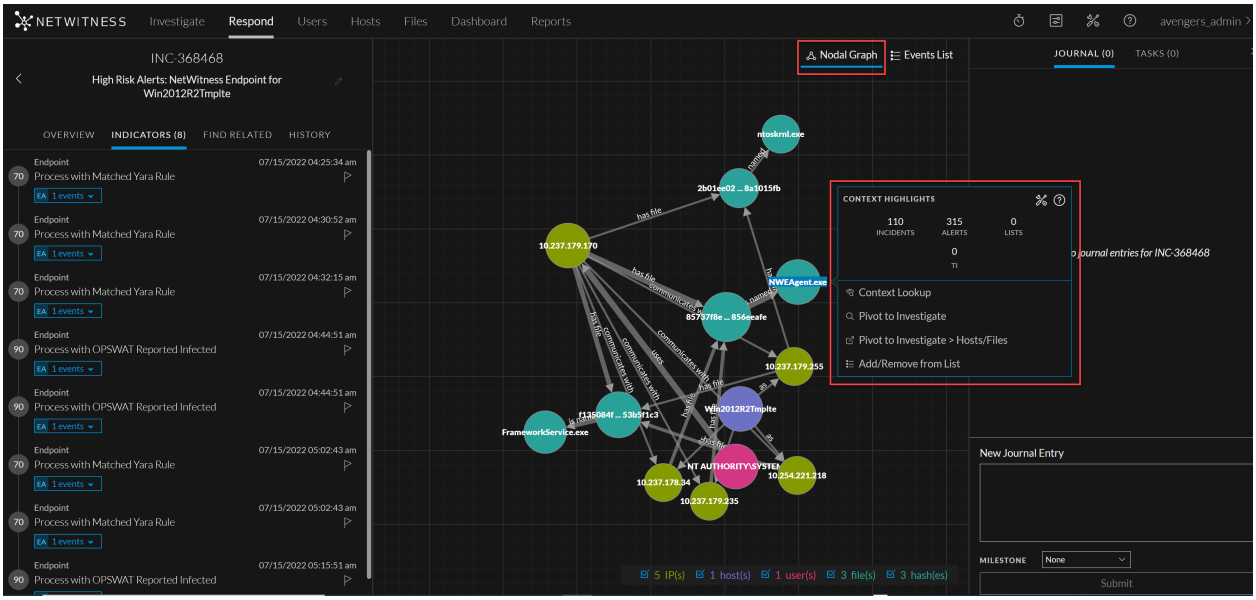


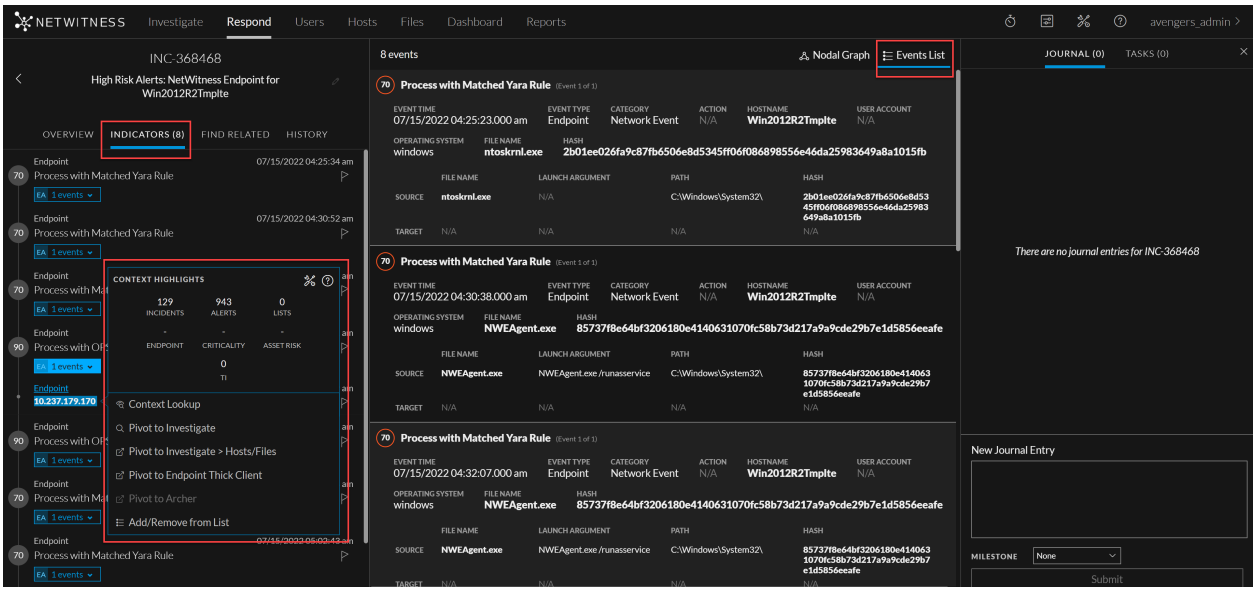


Respond View

Analysts have a unified way to interact with events metadata presented in the Respond view to perform actions or review contextual information.

On the Respond Indicators panel, Nodal Graph, and Events List view, analysts can use the left and right click options to view the unified panel data.



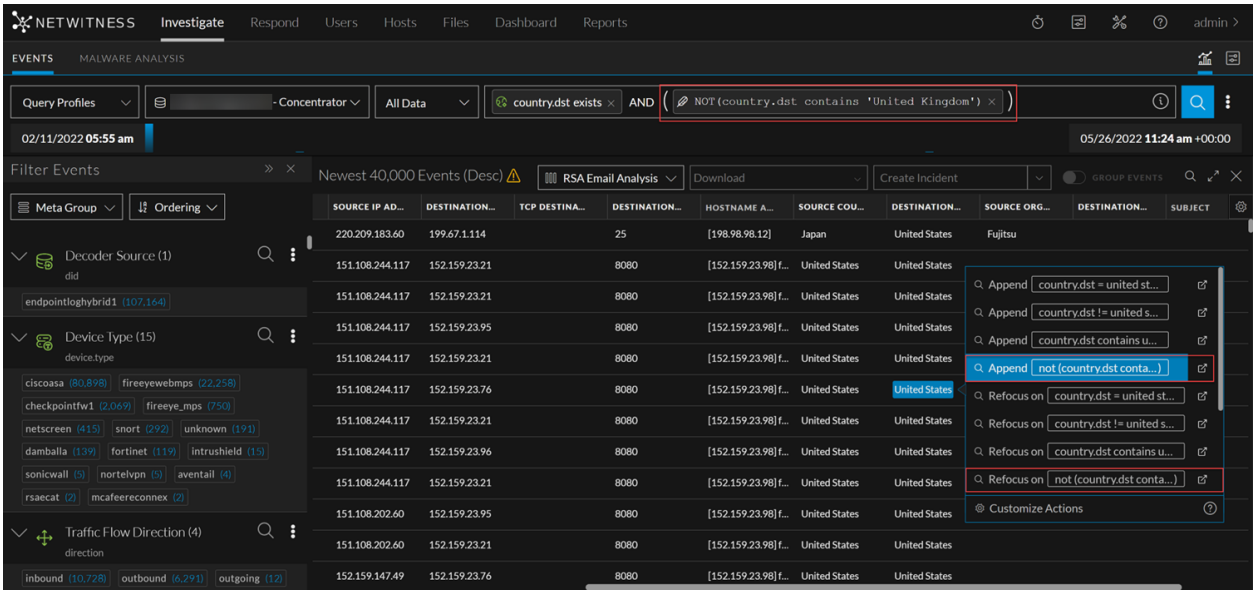


For more information, see NetWitness Platform Respond User Guide.

Enhanced Querying on Events View to Exclude any Specific Meta

Analysts can now exclude particular meta values while querying using the NOT(*meta* contains 'meta value') option available in the investigate unified panel. The specified meta value is removed from the query results when you use NOT(*meta* contains 'meta value') with **Append** or **Refocus** option on a specific meta value. This enhancement helps the analysts to view only the required data results in an optimized manner and conduct further investigation efficiently.

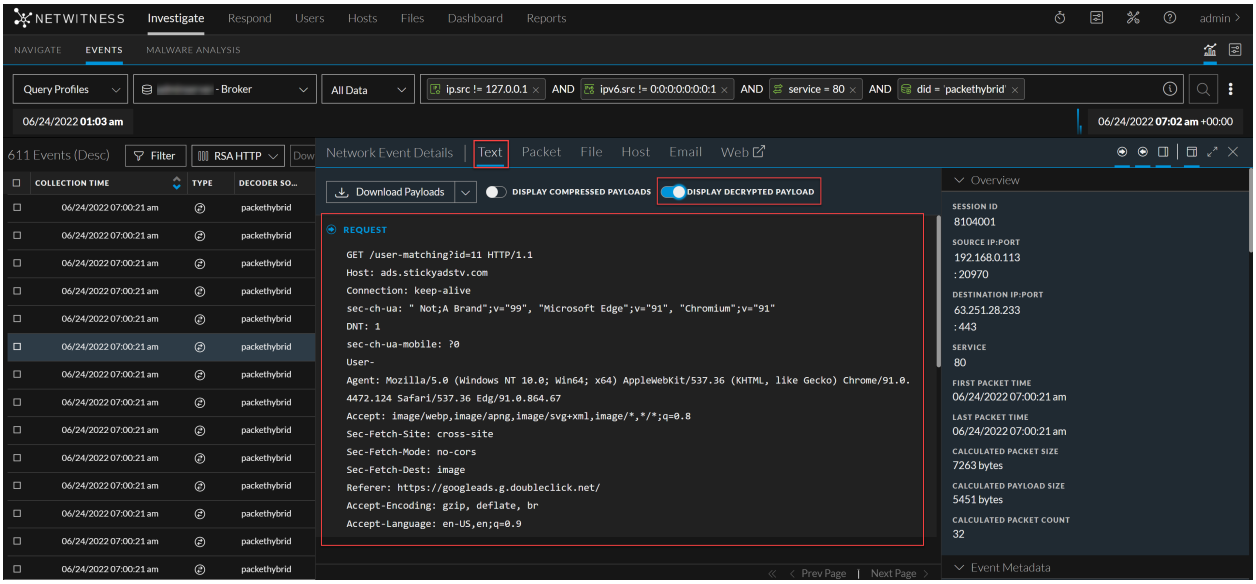
For more information, see the NetWitness Platform Investigate User Guide.



View Encrypted Data in Decrypted Format

Analysts can directly view encrypted data that has been decrypted by the decoder, thereby reducing time and effort in converting data into readable format. The analysts can enable using the **Display Decrypted Payload** toggle option in the **Events** > **Text** view.

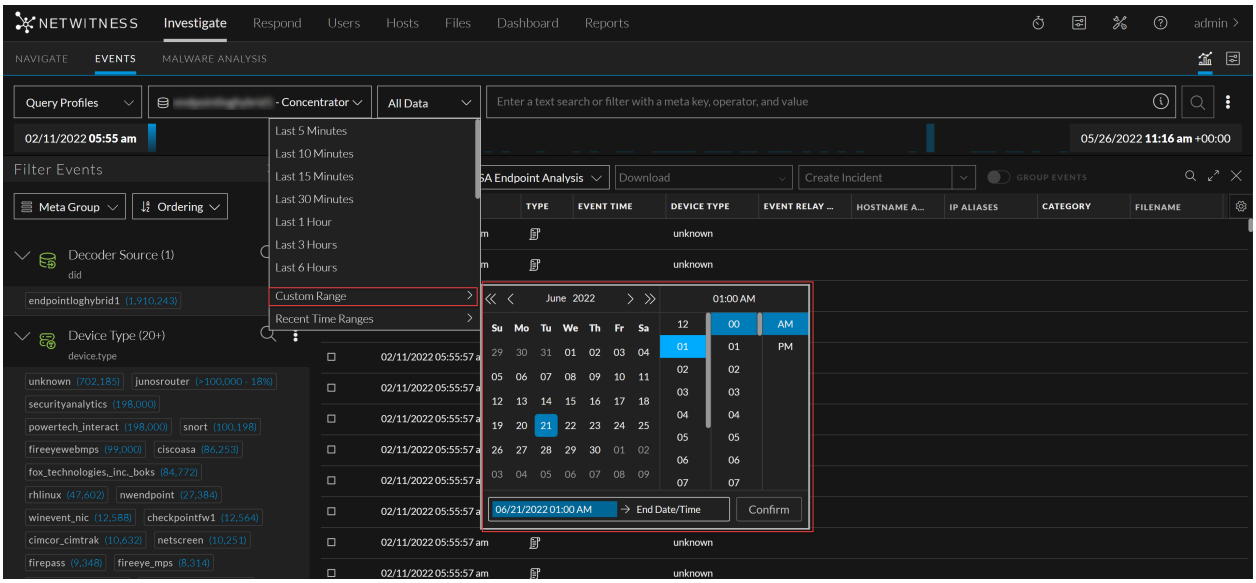
For more information, see the *Text Reconstruction* topic in the NetWitness Platform Investigate User Guide.



Select Custom Date and Time Range in the Events View

Analysts can set a custom range in the **Investigate** > **Events** view to select a specific time, date, month, and year using the calendar view that is displayed on clicking the **Custom Range** option. This enhancement helps the analysts to select date and time quickly and avoid manual intervention therefore avoiding human errors (typos).

For more information, see *Select a Time Range* topic in the NetWitness Platform Investigate User Guide.

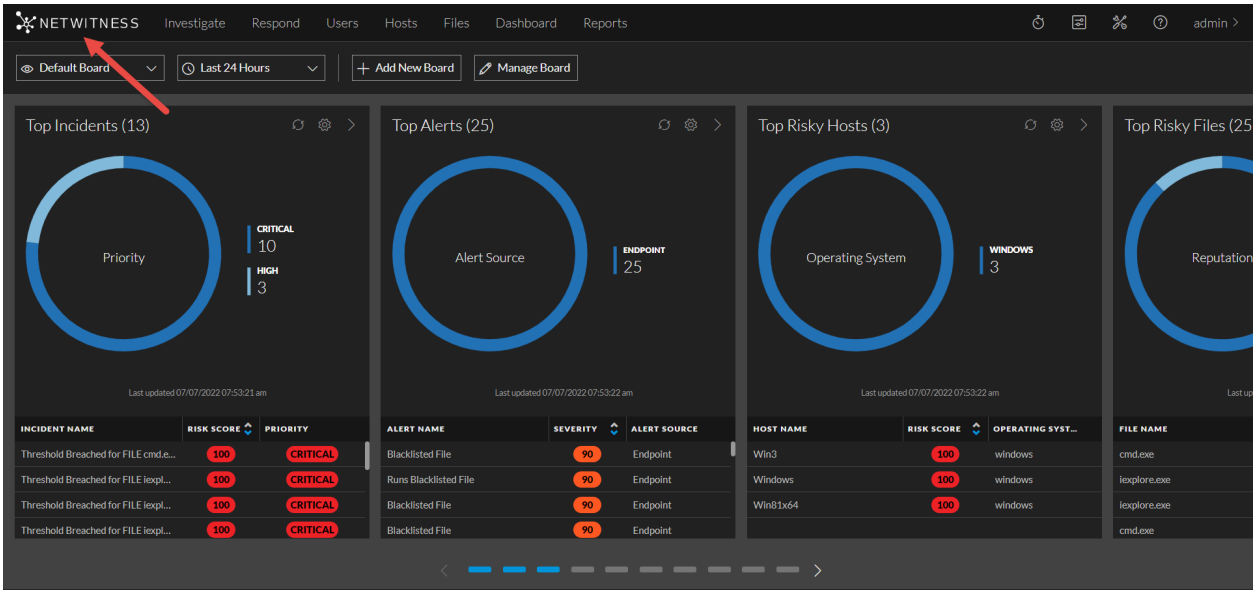


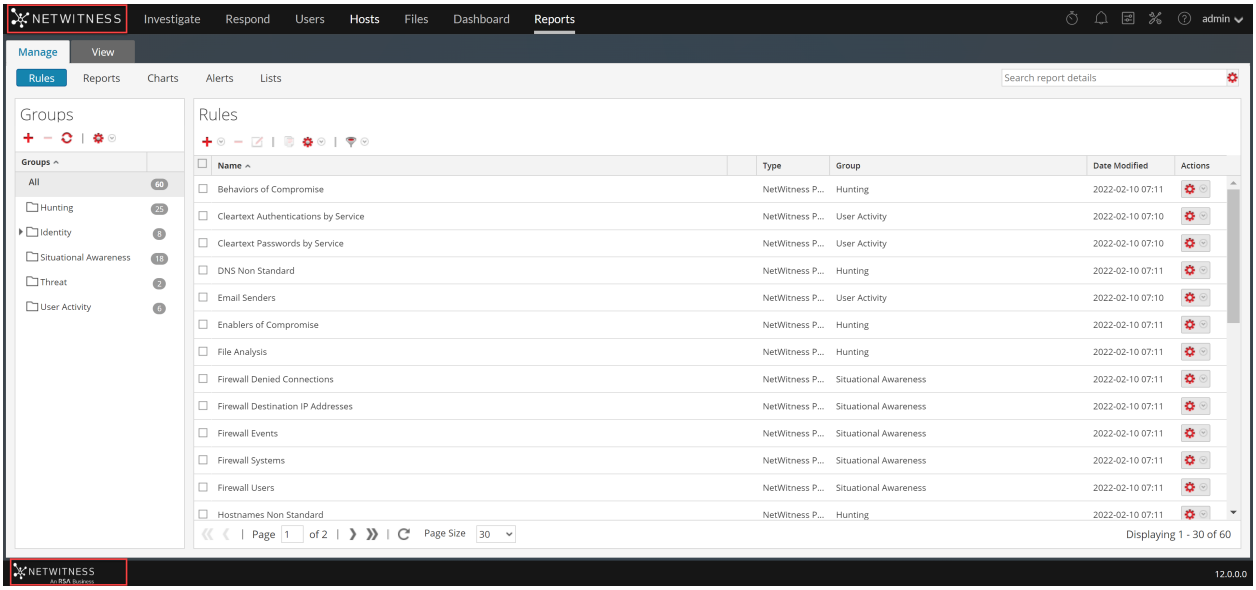
User Interface

The following section describes the new enhancements for the NetWitness user interface:

NetWitness User Interface Enhancements

- The 12.0.0.0 release includes the new NetWitness corporate logo. You can view the new logo in NetWitness Platform, which updates the identity of NetWitness as a trusted brand.
- As part of the repositioning, we are renaming our product as **NetWitness Platform XDR**. This change aims to simplify communications and improve our customers' understanding of how each product secures and protects within the NetWitness portfolio.





Endpoint Investigation

The following section describes the new enhancements for the Endpoint component:

Detection of removable Storage Devices

NetWitness Endpoint Agents are enhanced with the capabilities to detect and report removable storage devices. The Endpoint agents will detect and report when a removable storage device is plugged in or removed. This enhancement provides analysts with extended threat detection capabilities. For more information, see the NetWitness Endpoint User Guide.

Block Multiple File Hashes Using an Imported File

Administrators can import a file with a list of known file hashes that are not present in the environment and block them as soon as they are detected. This enhancement will help analysts to block multiple hashes without manual intervention.

Support for Arm-based Windows Machines

Administrators can install Endpoint agents on Arm-based Windows machines. This enhancement provides analysts with threat detection capabilities on more types of devices.

Download MFT from Multiple Hosts in One Step

Analysts can now download MFT(Master File Table) from multiple hosts on the Hosts list view in one step. This enhancement helps analysts download MFT without opening the Host details view of each host. For more information, See *Download Master File Table* topic on NetWitness Endpoint User Guide.

Customizable Maximum File Download Limits

The limit to the maximum number of file downloads on the Endpoint server is enhanced. On the explore page of an Endpoint server, Administrators can set the limit from 100 to 1000 files. For more information, see *Download Files Using Full Path or Wildcard* on NetWitness Endpoint User Guide.

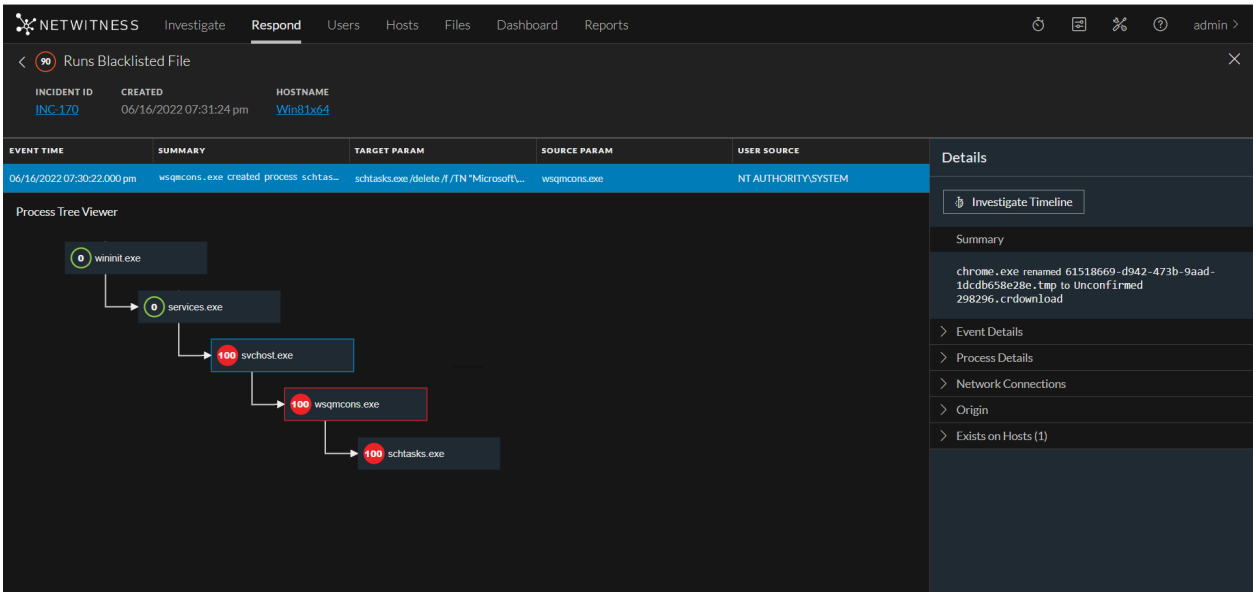
Redesigned Alert Details View for Endpoint Alerts in Respond

In the Respond view, the alert details view for Endpoint alerts shows end-to-end details about an alert. The details are presented in the form of a process tree along with a right panel that provides detailed information about the alert categorized into the following sections:

- **Summary**: A short summary of the alert.
- **Event Details**: Shows the directory, user, hash, signature, risk score, etc.
- **Process Details**: Shows the tactics, techniques, times and details about the targets.
- **Network Connections**: Shows any network connection established ten minutes before and till ten minutes after the alert triggered time.
- **Origin**: Shows how the selected file in the process tree is originated.
- **Exists on Hosts**: The host in which the selected file in the process tree exists.

Besides the above sections, the **Investigate Timeline** takes to the investigate view that has more detailed information.

For more information, see *Review Endpoint Alerts using Process Tree* on the NetWitness Respond User Guide.



Concentrator, Decoder, and Log Decoder Services

The following section describes the new enhancements for the Concentrator, Decoder, and Log Decoder components:

Log Parsing Enhancements

The following log parsing enhancements are made in 12.0.0.0 version. These are new elements that you use in the creation of a log parser:

New Selector Parsing Element Added to Dynamically Map Captured Values to a Meta Key

This will allow the log parser to automatically choose from two or more optional meta keys to assign to a parsed value depending upon the value of another meta key. Consider the following sample log snippet:

```
{ "Direction": "src", "Address": "1.2.3.4" }
{ "Direction": "dest", "Address": "5.6.7.8" }
```

In the above example, if the value of Direction is ”src”, then the preferred meta key to use for the value of Address would likely be **ip.src**. Conversely, if the value for Direction is ”dest”, then the meta key **ip.dst** might be preferred. This can now be achieved with the new **SELECTOR** log parsing element.

Support for Advanced Parsing Elements within CEF Parser and DataType

Support added to CEF parser for VARTYPE, SCANNED, DataType, and Selector parsing elements.

- Allows the CEF parser to take advantage of the fine parsing capabilities found in other parsers.

Dynamic parsing support including PARSERULESCAN added to DataType parsing element.

- Allows nesting of dynamic parsing elements (parse rules) from within an existing DataType.

Enhanced Network Decoder to Decrypt Incoming TLS 1.3 Packets

The enhanced network packet decryption capability helps inspect TLS 1.3 encrypted communications using ephemeral session keys. Administrators can configure Network Decoder to enable decryption of incoming TLS 1.3 network packets.

For more information, see the NetWitness Decoder Configuration Guide.

Event Stream Analysis (ESA)

The Event Stream Analysis is enhanced to reduce the time consumed for new rules deployment.

Improved ESA Rules Deployment

The ESA Rule Deployment has been enhanced with a new option to deploy the rules faster. If you want to push rule-related changes, you can quickly deploy the new rules by clicking the **Fast Deploy** option. For more information, see Alerting with ESA Correlation Rules User Guide.

Reports

The following section describes the new enhancements for the Reports component:

Build Rule View Enhancements

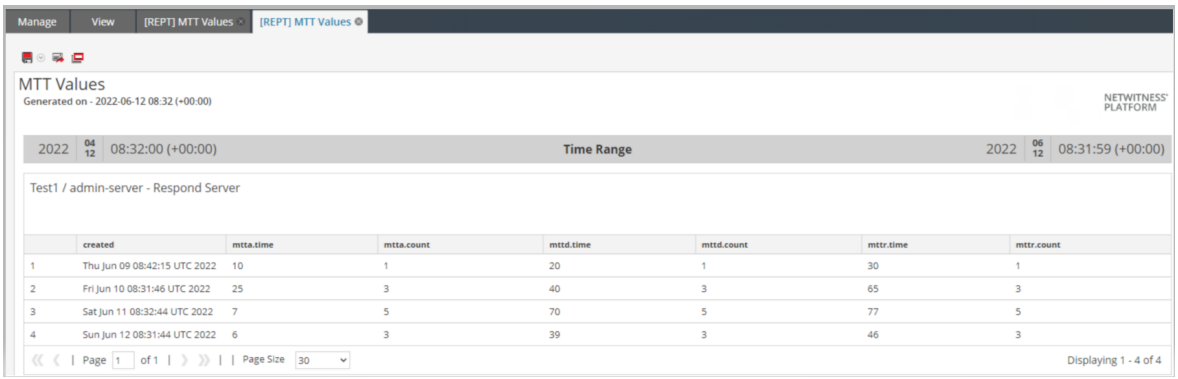
The **Build Rule** view is enhanced to help users view the following information in the report generated:

- The average time taken to assign the incident.
- The average time taken to complete the task.
- The average time taken to close the incident.

The following changes have been made in the **Build Rule** view:

1. Two new options are added in the **From** field:
   - **incidentStats**: The following metas are supported for **incidentStats**:
     a. **created**
     b. **mtta.time**: Displays the average time taken to acknowledge the incidents in a single day.
     c. **mtta.count**: Displays the number of incidents acknowledged in a single day.
     d. **mttd.count**: Displays the number of incidents detected in a single day.
     e. **mttd.time**: Displays the average time taken to detect the incidents in a single day.
     f. **mttr.time**: Displays the average time taken to resolve the incidents in a single day.
     g. **mttr.count**: Displays the number of incidents resolved in a single day.

     These metas are displayed in the report generated. Refer the following figure.

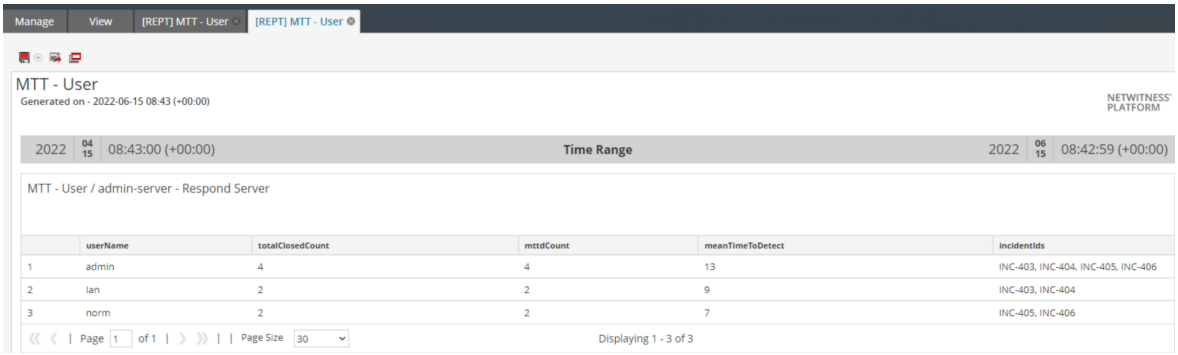


   - **incidentUserStats**: The following metas are supported for **incidentUserStats**:
     a. **userName**: Displays the assignee's or the user's ID for the associated user stats.
     b. **totalClosedCount**: Displays the total number of Incidents closed by the assignee till date.
     c. **meanTimeToDetect**: Displays the average time taken by the user to detect the incidents in the time range selected.

d. **mttdCount**: Displays the count of incidents contributing to the MTTD value computed.

e. **incidentIds**: Displays the list of incident IDs closed by the user during the time range selected.

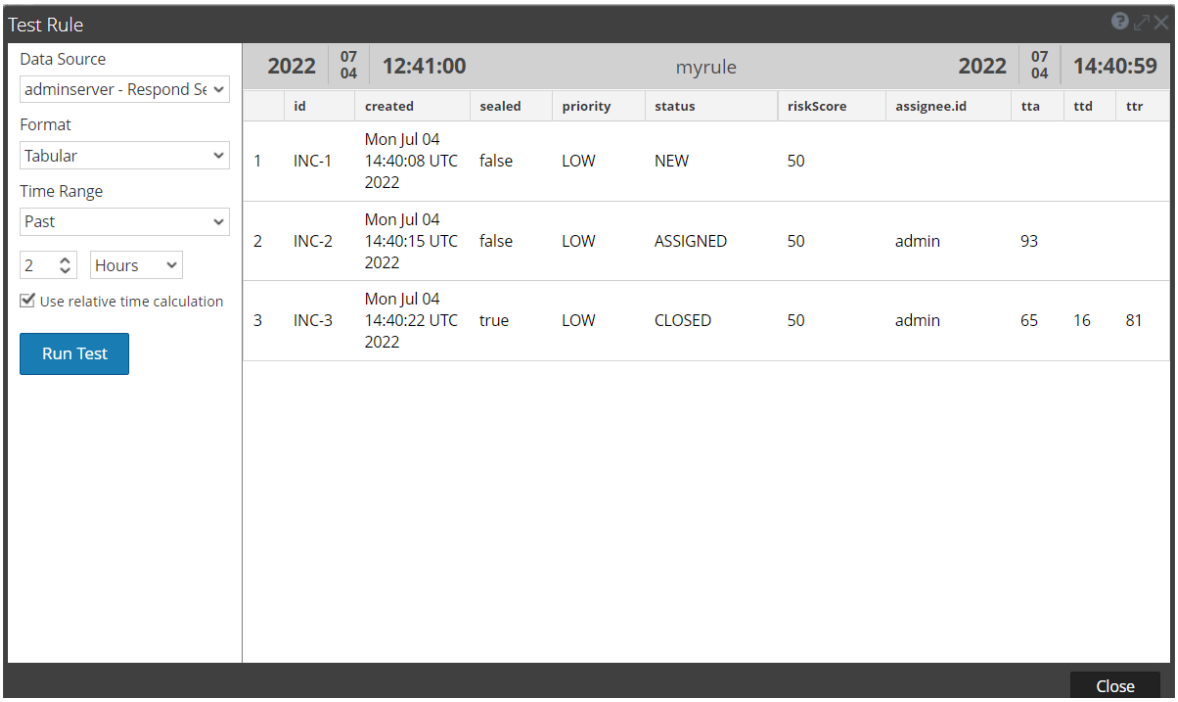
These metas are displayed in the report generated. Refer the following figure.



2. New metas are added for **incident**. The newly added metas are as shown below:

- **assignee.id**
- **tta**(Time to Acknowledge): Displays the time taken to assign an Incident after creating it.
- **ttd**(Time to Detect): Displays the time taken for completing the task after the Incident is assigned.
- **ttr**(Time to Resolve): Displays the time taken for closing the task after the Incident is created.

These metas are populated on the **Test Rule** view. Refer the following figure.



For more information, see the *Create a Rule Using Respond Data Source* topic in the NetWitness Reporting User Guide.

Fixed Issues

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the NetWitness® Platform Known Issues list on NetWitness Community Portal.

Administration Fixes

Tracking Number	Description
ASOC-114808	Multiple operations fail after you enable logging for CRUD operation on app rules and use separate API for ADD, DELETE, and UPDATE.
ASOC-113813	The Jobs **(Admin > System > Jobs)** with lengthy queries take a long time to load. As a result, the load time of the Jobs page is affected.

Endpoint Fixes

Tracking Number	Description
SACE-17157	Network adapter in promiscuous state is not identified due to querying wrong wmi namespace by NetWitness agent.
ASOC-113849	Failed icon is displayed beside the agent version (**Hosts> Agent History**) when there is a time difference between agent and server.

Respond Fixes

Tracking Number	Description
ASOC-115196	Aggregation syntax count is not displayed in the report, when you try to create a report with metas such as alert.name, alert.severity,count (alert.numEvents).

Core Services (Broker, Concentrator, Decoder, Archiver) Fixes

Tracking Number	Description
ASOC-114900	Brotil data fails to decompress in Events page (**Investigate> Events**). When exporting data, it is decompressed but on Events page invalid data is displayed.
ASOC -115052	Due to the large size of incoming logs aggregation fails and archiver service crashes. The mem page issue occurs if sessions to be aggregated from log decoder are with large packet andlog sizes.

Reporting Engine Fixes

Tracking Number	Description
ASOC -115232	NetWitness Weekly Scheduled Reports run on a different day after conversion to UTC flows into either the previous or next day for time zones other than the UTC time zone

Log Collection Fixes

Tracking Number	Description
ASOC-120851	After upgrading to 11.7.1.0, WinRM log collection is interrupted due to the conflict in the internal artifact. As a result, logs are not collected from the WinRM server.

End of Life Functionality

The following table provides information on end of life functionality, features and hardware in NetWitness 12.0.0.0 or later releases.

End of Life Functionality and Features in 12.0.0.0 or higher releases

Feature	Notes
Dell Series 4 and Series 4s Hardware	As the Dell S4 and S4s appliances reached the end of life (EOL) in June 2021, we recommend that you not perform any installation or upgrade activities on these and upgrade to new hardware.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform Master Table of Contents	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.0 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.0.0.0 Upgrade Guide	https://community.netwitness.com//t5/rsa-netwitness-platform-staged/upgrade-guide-for-11-7-1/ta-p/658666

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here:https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the guides.
- See also RSA NetWitness® Platform Blog Posts.
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Support

If you contact NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact RSA NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW Update	update.netwitness.com
LiveUi	live.netwitness.com

Build Numbers

The following table lists the build numbers for various components of NetWitness 12.0.0.0

Component	Version Number
NetWitness Audit Plugins	rsa-audit-plugins-12.0.0.0-4762.5.8853c5bef.el7.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Broker	rsa-nw-broker-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.0.0.1-2208052108.5.104cf25.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.0.0.0-220531042629.5.b236ead.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-12.0.0.0-220426021902.5.dc28ce9.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.0.0.0-220613050521.5.b986911.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.0.0.0-220610051650.5.57a3c20.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.0.0.0-12536.5.ee5a55cf6.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.0.0.1-2208060358.5.3df31a1.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-12.0.0.0-2206211619.5.3fe862e.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.0.0.0-220610063852.5.b91f656.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.0.0.0-220620061620.5.ea8ba76.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.0.0.0-220609130615.5.71ca677.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-12.0.0.0-220607015824.5.dbfcf19.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.0.0.1-220806042518.5.2c3da62.el7.centos.noarch.rpm

NetWitness License Server	rsa-nw-license-server-12.0.0.0-220412123008.5.1fb53c8.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.0.0.0-15032.5.5e731802a.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.0.0.0-220520044551.5.56297e2.el7.centos.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-12.0.0.0-220530065358.5.24033a9.el7.centos.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.0.0.0-220531093544.5.ed07d6c.el7.centos.noarch.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-12.0.0.0-2205190541.5.c20bc1d.el7.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.0.0.0-5948.5.378a71f6b.el7.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.0.0.0-220613050612.5.15a626b.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-12.0.0.0-2206021205.5.47aad12.el7.noarch.rpm
NetWitness SDK	rsa-nw-sdk-11.6.0.0-11374.5.fe9457e29.el7.x86_64.rpm
NetWitness Security Server	rsa-nw-security-server-12.0.0.0-220624043254.5.b9a8a8f.el7.centos.noarch.rpm
NetWitness Source Server	rsa-nw-source-server-12.0.0.0-220623003834.5.d4e49fb.el7.centos.noarch.rpm
NetWitness User Interface	rsa-nw-ui-12.0.0.1-220806005807.5.e33efada87.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.0.0.0-12540.5.9f874c638.el7.x86_64.rpm
NetWitness SA Tools	rsa-sa-tools-12.0.0.1-2208060720.5.4d4a622.el7.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-12.0.0.0-4762.5.8853c5bef.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.0.0.0-4762.5.8853c5bef.el7.x86_64.rpm
NetWitness Windows Legacy Log Collector	NWLegacyWindowsCollector-12.0.0.1-15036.5.056fd2393.exe

Revision History

Date	Description
August 2022	General Availability