RSA NETWITNESS® SUITE

Cb Response Interoperability

Trademarks

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION 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.

October 2018

Contents

RSA NetWitness Interoperability with Cb Response

Cb Response provides complete visibility, fast analysis and a remote remediation toolset to enable fast end-to-end incident response. Cb Response is purpose-built for enterprise SOC and IR teams. It offers a streamlined UI that is built for speed, unlimited historical data retention and unlimited scaling to fit even the largest enterprises.

The following table lists the available Interops available with Carbon Black, and the RSA NetWitness component required for each.

	RSA NetWitness Component	
Feature	**Logs/SIEM**	**Packet**
Parsing of CB Logs	X	🟥
Populate CB Dashboard	X	🟥
Right-Click from NW to CB	X	X
Ingest CB IOC feeds	X	X

The **Logs/SIEM** column indicates that the RSA NetWitness system should have Log Decoder present in the ecosystem for the corresponding interop to work.

Interoperability Between RSA NetWitness and Cb Response

RSA NetWitness supports the following interoperability with Cb Response:

- Receive Cb Response Logs into RSA NetWitness
- RSA NetWitness Investigation to Cb Response UI on:
  - Filename/Directory
  - Device IP
  - Hostname
- Pivot from RSA NetWitness Investigation to Cb Live Response
- Pivot on hostname from RSA NetWitness Investigation to Cb Response Isolate Host
- Pivot from RSA NetWitness to the Cb Response File Delete process
- Create a Cb Response Interop Dashboard in RSA NetWitness
- Create RSA NetWitness feeds from CbAPI Response Feeds

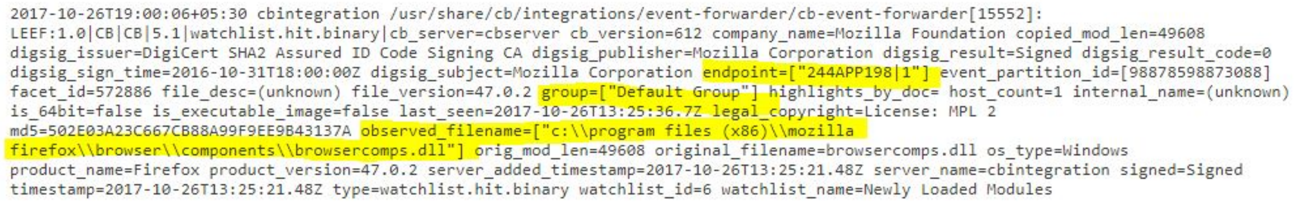
Known Interoperability Issues

Log File Delimiter

The RSA carbonblack parser is dependent on logs being sent using a tab character as the delimiter. If Cb Response logs are sent to RSA NetWitness using other delimiters (for example the space character), parsing of the logs will not be done correctly.

Log File Values Inside Braces

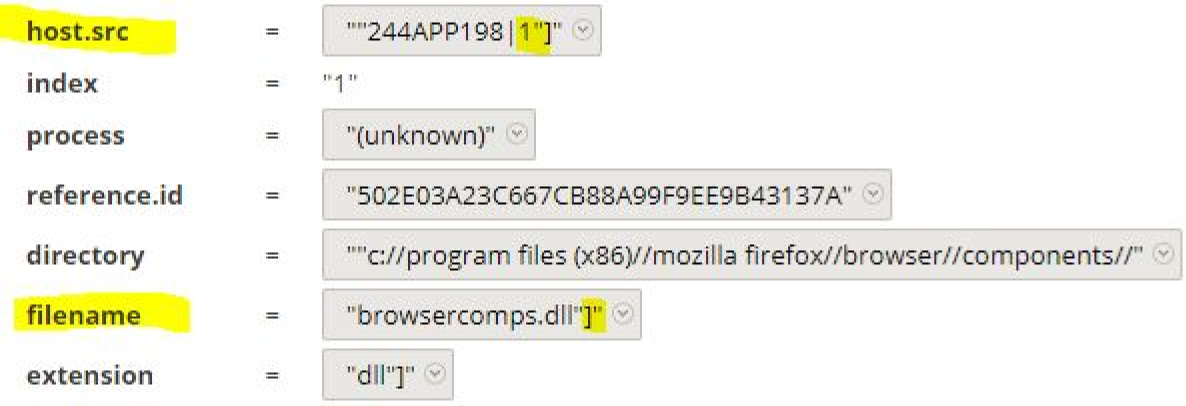
Cb occasionally outputs logs with braces, which enter RSA NetWitness in a ["<value>"] format, as shown in the following highlighted text:



```
2017-10-26T19:00:06+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-forwarder[15552]:
LEEF:1.0|CB|CB|5.1|watchlist.hit.binary|cb_server=cbserver cb_version=612 company_name=Mozilla Foundation copied_mod_len=49608
digsig_issuer=DigiCert SHA2 Assured ID Code Signing CA digsig_publisher=Mozilla Corporation digsig_result=Signed digsig_result_code=0
digsig_sign_time=2016-10-31T18:00:00Z digsig_subject=Mozilla Corporation endpoint=["244APP198|1"] event_partition_id=[98878598873088]
facet_id=572886 file_desc=(unknown) file_version=47.0.2 group=["Default Group"] highlights_by_doc= host_count=1 internal_name=(unknown)
is_64bit=false is_executable_image=false last_seen=2017-10-26T13:25:36.7Z legal_copyright=License: MPL 2
md5=502E03A23C667CB88A99F9EE9B43137A observed_filename=["c:\\program files (x86)\\mozilla
firefox\\browser\\components\\browsercomps.dll"] orig_mod_len=49608 original_filename=browsercomps.dll os_type=Windows
product_name=Firefox product_version=47.0.2 server_added_timestamp=2017-10-26T13:25:21.48Z server_name=cbintegration signed=Signed
timestamp=2017-10-26T13:25:21.48Z type=watchlist.hit.binary watchlist_id=6 watchlist_name=Newly Loaded Modules
```

This should be fixed in an upcoming Cb Response release.

When parsed, the corresponding meta values have the **"]** characters as shown here:



host.src	=	""244APP198|1"]"
index	=	"1"
process	=	"(unknown)"
reference.id	=	"502E03A23C667CB88A99F9EE9B43137A"
directory	=	""c://program files (x86)//mozilla firefox//browser//components//"
filename	=	"browsercomps.dll"]"
extension	=	"dll"]"

Also note that the endpoint is translated into the **host.src** meta key. In the previous example, the log has the endpoint value:

`endpoint=["244app183|1"]`

This is parsed as the following:

`host.src = "244app183|1""]`

This means that whenever an external source is used for hostname, the Cb UI will throw an error when conducting a search. So the customer needs to remove in the URL everything after **244app183** (removing **|1"]**). This is also true for the **filename** meta value: the customer needs to remove the **"]** from the URL in Cb Response.

So, for hostname searches, if **host.src** contains `<hostname>|<number>`, the source URL needs to be editing in Cb Response. The procedure is as follows:

1. Do the External Lookup from the RSA NetWitness Investigation view.
2. In the Cb Response UI, remove anything after hostname in the URL or search text box. For example, if the search text box contains **244app183|1**, remove the **|1** characters. If you do not remove the extra characters from the search string, Cb Response throws an error.
3. Perform the search. If you removed the extra characters, the search runs successfully.

Note: The same procedure is necessary when doing external lookups on the filename.

Receive Cb Response Logs into RSA NetWitness

RSA NetWitness can receive syslog alerts. Cb Response can forward logs and alerts in JSON or LEEF format syslog. Cb Response sends this data as Syslog to the RSA NetWitness Log Decoder. This is a 2-part process:

I. Configure Cb Response to send data to RSA NetWitness

II. Use the new carbonblack parser in RSA NetWitness to extract meta values.

Configure Cb Response to send data to RSA NetWitness

To configure the Event Forwarder in Github:

1. Log into github.
2. Download the https://github.com/carbonblack/cb-event-forwarder.
3. Go to your Carbon Black server.
4. Follow the instructions in the github for cb-event-forwarder and install.
5. Edit the configuration file, `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf`, as follows:

   ```
   output_type=syslog
   output_format=leef
   syslogout=tcp:NW Log Decoder/VLC-IP:514
   ```

   where ***<NW Log Decoder/VLC-IP>*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector. For example:

   ```
   syslogout=udp:10.31.246.203:514
   ```

6. In `cb-event-forwarder.conf`, there is a section on Raw Sensor (endpoint) Events, Watchlist Hits, Feed Hits, Alert Events, Binary Observed Events and Binary Upload Events. Check the **Appendix > Cb Config** section of the file, and ensure you see the values set to ALL as shown here:

   ```
   events_raw_sensor=ALL

   events_watchlist=ALL

   events_feed=ALL

   events_alert=ALL

   events_binary_observed=ALL

   events_binary_upload=ALL
   ```

7. Restart and generate events.

To see examples of logged events, see the Log Samples section in the Appendix.

Use the carbonblack Parser

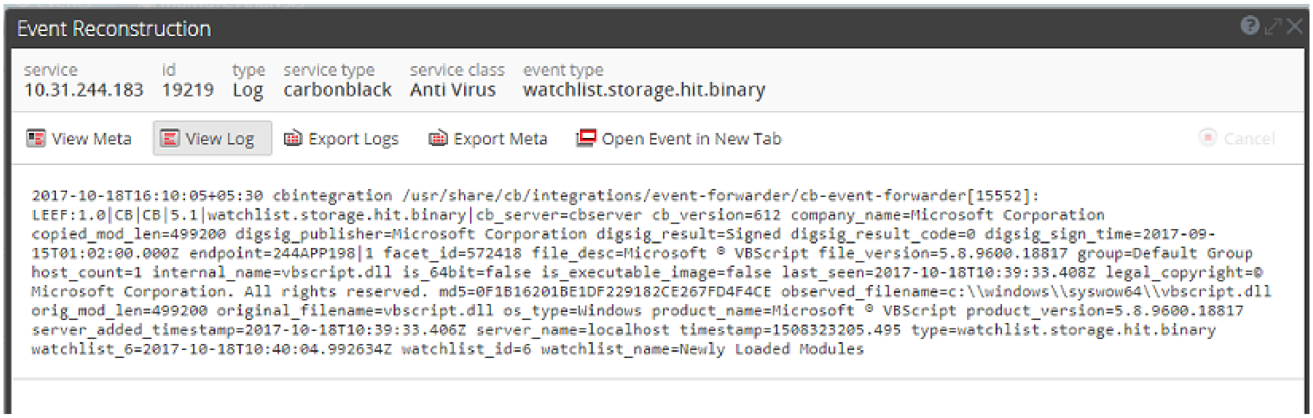
To parse logs using the carbonblack parser in RSA NetWitness:

1. SSH into the RSA NetWitness Log Decoder with Administrative Credentials.
2. Go to `/etc/netwitness/ng/envision/etc/devices`, and copy the **carbonblack** file directory provided into this folder. The directory contains the following files:
   - carbonblack.ini
   - carbonblackmsg.xml
3. Restart the **nwlogdecoder** service by running the following commands:

   ```
   stop nwlogdecoder
   start nwlogdecoder
   ```

4. Start generating events in Carbon Black. The cb-event-forwarder will start sending logs.

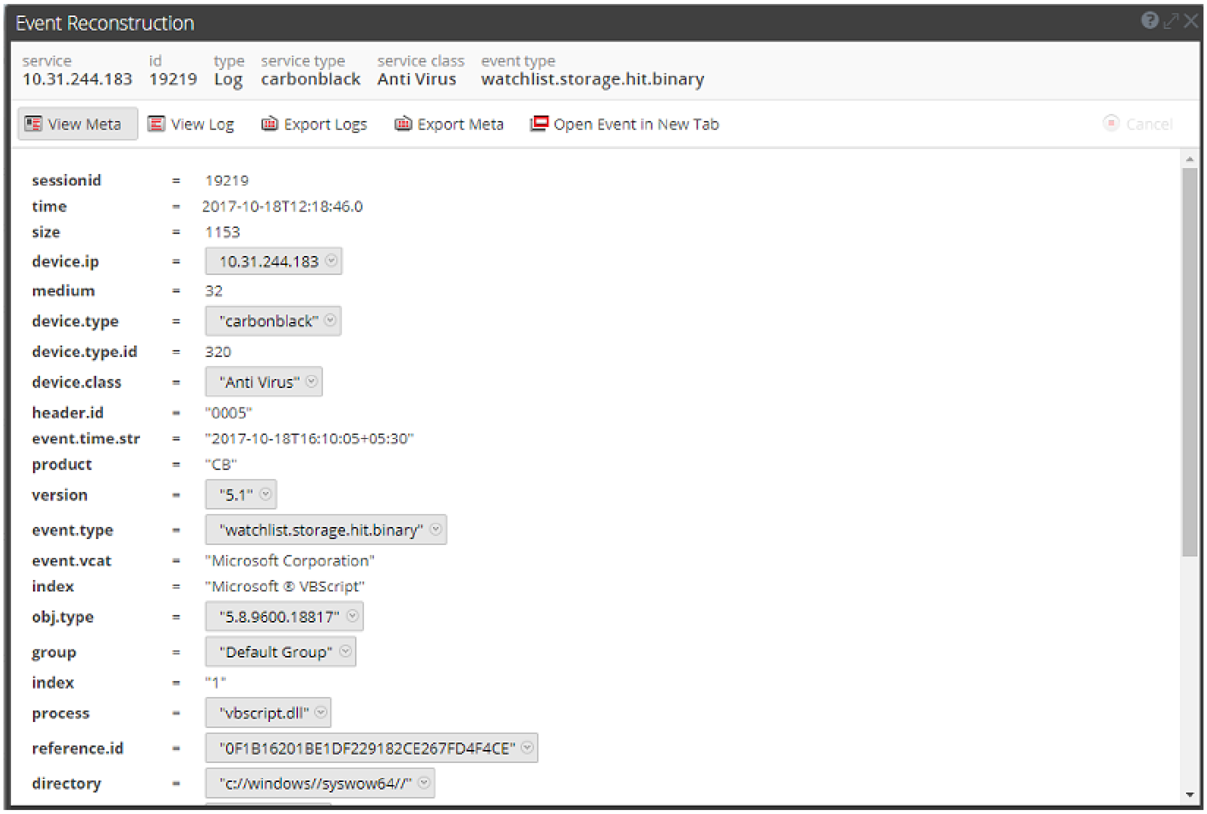
Sample screen showing logs as sent to RSA NetWitness, from Cb Response in LEEF format:



service	id	type	service type	service class	event type
10.31.244.183	19219	Log	carbonblack	Anti Virus	watchlist.storage.hit.binary

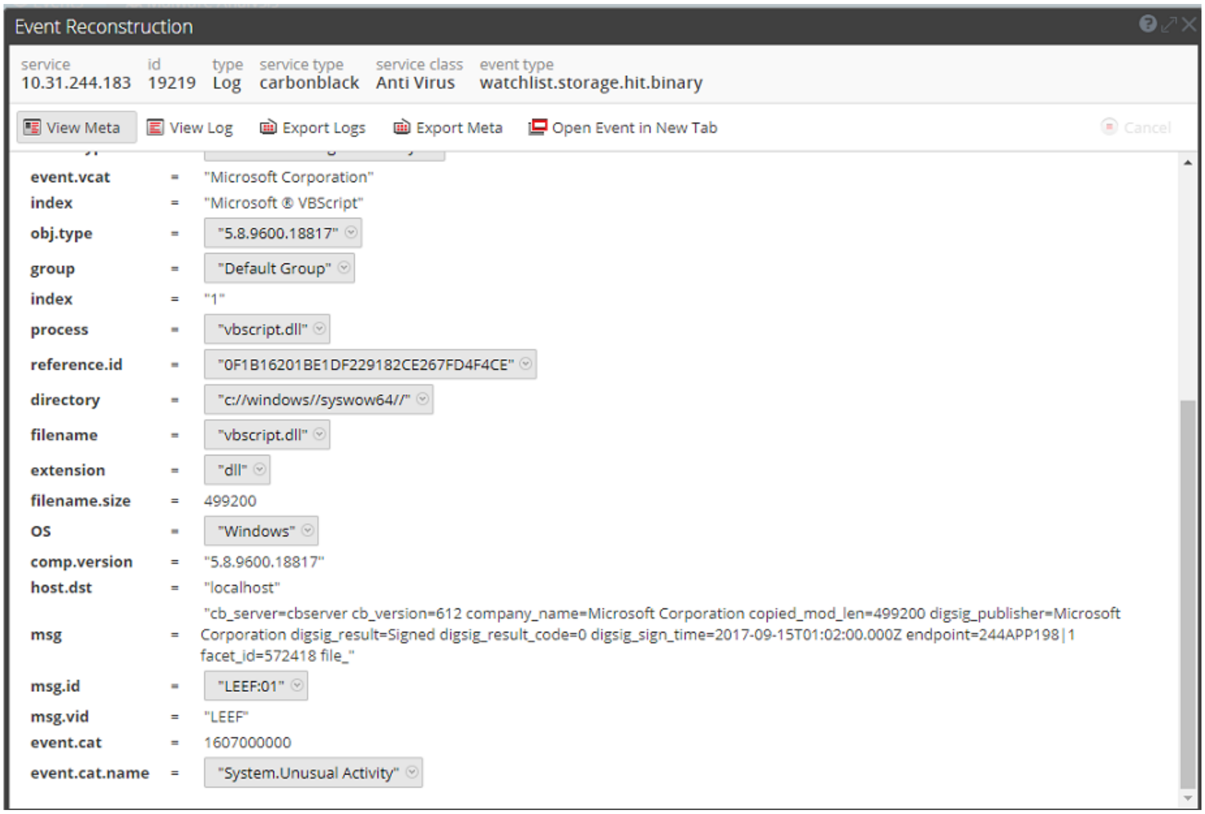
```
2017-10-18T16:10:05+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-forwarder[15552]:
LEEF:1.0|CB|CB|5.1|watchlist.storage.hit.binary|cb_server=cbserver cb_version=612 company_name=Microsoft Corporation
copied_mod_len=499200 digsig_publisher=Microsoft Corporation digsig_result=Signed digsig_result_code=0 digsig_sign_time=2017-09-
15T01:02:00.000Z endpoint=244APP198|1 facet_id=572418 file_desc=Microsoft ® VBScript file_version=5.8.9600.18817 group=Default Group
host_count=1 internal_name=vbscript.dll is_64bit=false is_executable_image=false last_seen=2017-10-18T10:39:33.408Z legal_copyright=©
Microsoft Corporation. All rights reserved. md5=0F1B16201BE1DF229182CE267FD4F4CE observed_filename=c:\\windows\\syswow64\\vbscript.dll
orig_mod_len=499200 original_filename=vbscript.dll os_type=Windows product_name=Microsoft ® VBScript product_version=5.8.9600.18817
server_added_timestamp=2017-10-18T10:39:33.406Z server_name=localhost timestamp=1508323205.495 type=watchlist.storage.hit.binary
watchlist_6=2017-10-18T10:40:04.992634Z watchlist_id=6 watchlist_name=Newly Loaded Modules
```

Sample screens showing the information extracted from the above logs and parsed by the carbonblack parser:



service	id	type	service type	service class	event type
10.31.244.183	19219	Log	carbonblack	Anti Virus	watchlist.storage.hit.binary

```
sessionid       =  19219
time            =  2017-10-18T12:18:46.0
size            =  1153
device.ip       =  10.31.244.183
medium          =  32
device.type     =  "carbonblack"
device.type.id  =  320
device.class    =  "Anti Virus"
header.id       =  "0005"
event.time.str  =  "2017-10-18T16:10:05+05:30"
product         =  "CB"
version         =  "5.1"
event.type      =  "watchlist.storage.hit.binary"
event.vcat      =  "Microsoft Corporation"
index           =  "Microsoft ® VBScript"
obj.type        =  "5.8.9600.18817"
group           =  "Default Group"
index           =  "1"
process         =  "vbscript.dll"
reference.id    =  "0F1B16201BE1DF229182CE267FD4F4CE"
directory       =  "c://windows//syswow64//"
```



service	id	type	service type	service class	event type
10.31.244.183	19219	Log	carbonblack	Anti Virus	watchlist.storage.hit.binary

```
event.vcat      =  "Microsoft Corporation"
index           =  "Microsoft ® VBScript"
obj.type        =  "5.8.9600.18817"
group           =  "Default Group"
index           =  "1"
process         =  "vbscript.dll"
reference.id    =  "0F1B16201BE1DF229182CE267FD4F4CE"
directory       =  "c://windows//syswow64//"
filename        =  "vbscript.dll"
extension       =  "dll"
filename.size   =  499200
OS              =  "Windows"
comp.version    =  "5.8.9600.18817"
host.dst        =  "localhost"
msg             =  "cb_server=cbserver cb_version=612 company_name=Microsoft Corporation copied_mod_len=499200 digsig_publisher=Microsoft
                   Corporation digsig_result=Signed digsig_result_code=0 digsig_sign_time=2017-09-15T01:02:00.000Z endpoint=244APP198|1
                   facet_id=572418 file_"
msg.id          =  "LEEF:01"
msg.vid         =  "LEEF"
event.cat       =  1607000000
event.cat.name  =  "System.Unusual Activity"
```

RSA NetWitness Investigation to Cb Response UI

Once RSA NetWitness has parsed the events, as described in the previous section, analysts can search into the Carbon Black UI. Analysts can pivot from meta information in RSA NetWitness to the Carbon Black search screen with filename, IP, or hostname data from a RSA NetWitness Investigation screen used as the starting drill-point into the Carbon Black dataset. This enables focused, time-based searches of the Carbon Black dataset instead of broad IP-only searches.

We use the context actions integration to configure RSA NetWitness-to-Carbon Black integration. Each of the integrations provide a different field or result in Carbon Black. For example, using the **Search Carbon Black - filename** action looks up the `filename` key in Carbon Black.

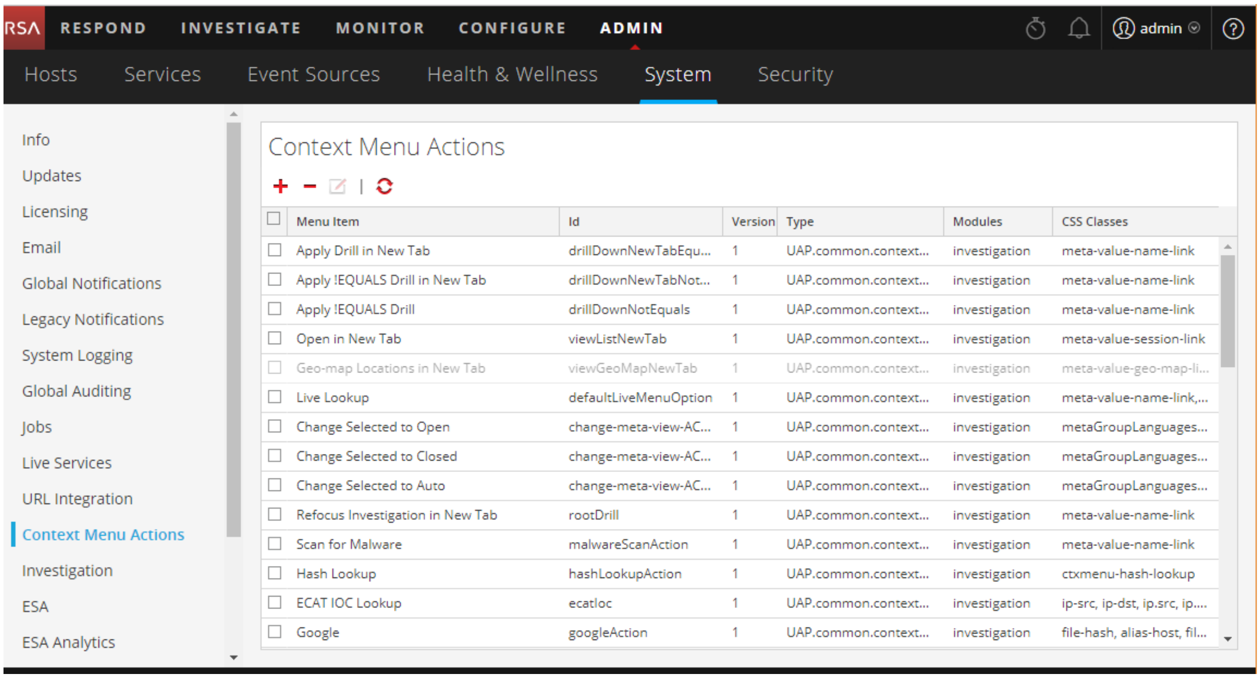
The following sections describe how to create context actions in RSA NetWitness Platform and then perform an external lookup using the following meta keys:

- Filename/Directory
- IP Address
- Hostname

Add a Context Menu Action for Filename/Directory

1. Log onto the RSA NetWitness Platform UI.
2. Go to **ADMIN** > **System** > **Context Menu Actions**.

   The Context Menu Actions screen appears.



Context Menu Actions

□	Menu Item	Id	Version	Type	Modules	CSS Classes
□	Apply Drill in New Tab	drillDownNewTabEqu...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill in New Tab	drillDownNewTabNot...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill	drillDownNotEquals	1	UAP.common.context...	investigation	meta-value-name-link
□	Open in New Tab	viewListNewTab	1	UAP.common.context...	investigation	meta-value-session-link
□	Geo-map Locations in New Tab	viewGeoMapNewTab	1	UAP.common.context...	investigation	meta-value-geo-map-li...
□	Live Lookup	defaultLiveMenuOption	1	UAP.common.context...	investigation	meta-value-name-link,...
□	Change Selected to Open	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Closed	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Auto	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Refocus Investigation in New Tab	rootDrill	1	UAP.common.context...	investigation	meta-value-name-link
□	Scan for Malware	malwareScanAction	1	UAP.common.context...	investigation	meta-value-name-link
□	Hash Lookup	hashLookupAction	1	UAP.common.context...	investigation	ctxmenu-hash-lookup
□	ECAT IOC Lookup	ecatIoc	1	UAP.common.context...	investigation	ip-src, ip-dst, ip.src, ip....
□	Google	googleAction	1	UAP.common.context...	investigation	file-hash, alias-host, fil...

3. Add the Carbon Black Context Menu Action.

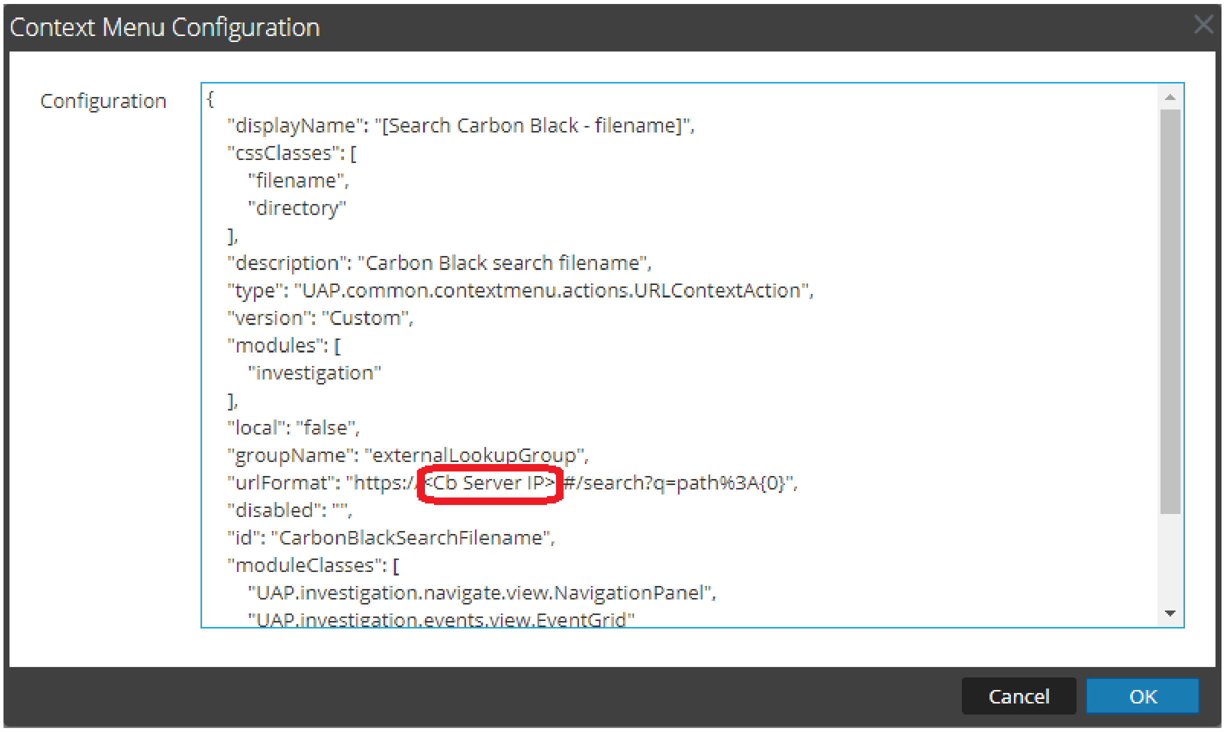
   a. In the toolbar, click +.

      The Context Menu Configuration dialog box appears.

   b. Paste the following text into the Context Menu Configuration dialog box :

```
{

      "displayName": "[Search Carbon Black - filename]",
      "cssClasses": [
         "filename",
         "directory"
      ],

      "description": "Carbon Black search filename",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "https://<Cb Server IP>/#/search?q=path%3A{0}",
      "disabled": "",
      "id": "CarbonBlackSearchFilename",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
        "openInNewTab": "true",
        "order":"16"

}
```

The screen should look similar to this (without the red box):



```
{
   "displayName": "[Search Carbon Black - filename]",
   "cssClasses": [
      "filename",
      "directory"
   ],
   "description": "Carbon Black search filename",
   "type": "UAP.common.contextmenu.actions.URLContextAction",
   "version": "Custom",
   "modules": [
      "investigation"
   ],
   "local": "false",
   "groupName": "externalLookupGroup",
   "urlFormat": "https://<Cb Server IP>/#/search?q=path%3A{0}",
   "disabled": "",
   "id": "CarbonBlackSearchFilename",
   "moduleClasses": [
      "UAP.investigation.navigate.view.NavigationPanel",
      "UAP.investigation.events.view.EventGrid"
```

c. Edit the following line (shown outlined in red in the image above), replacing **<Cb Server IP>** with the IP address of your Carbon Black server:

```
"urlFormat": "https://<Cb Server IP>/#/search?q=path%3A{0}",
```

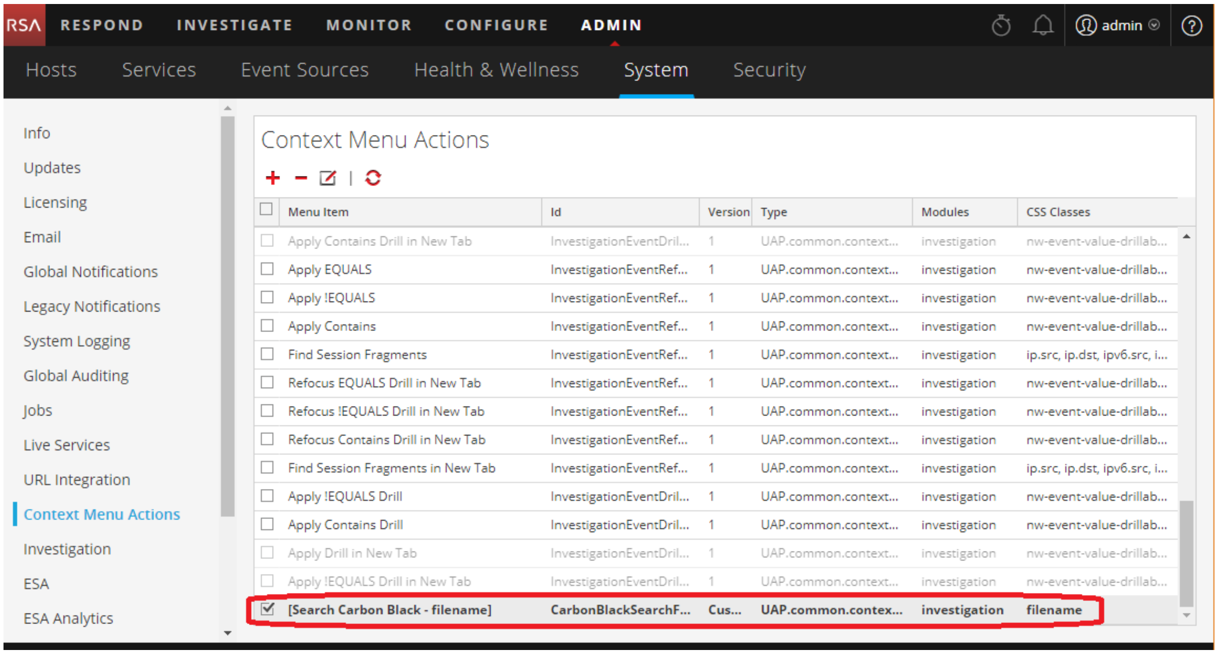
For example:

```
"urlFormat": "https://10.100.32.8/#/search?q=path%3A{0}",
```

> **Note:** If you are not using SSL, change **https** to **http**.

d. Click OK.

The context menu action is added to the end of the list, as shown below (outlined in red):



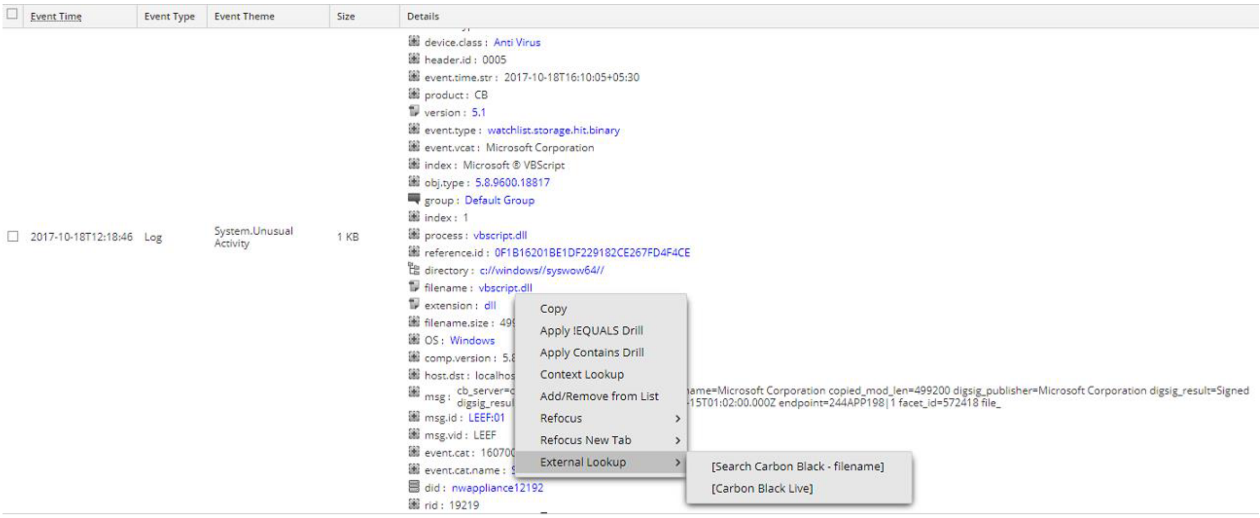
Context Menu Actions

□	Menu Item	Id	Version	Type	Modules	CSS Classes
□	Apply Contains Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply EQUALS	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply !EQUALS	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply Contains	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Find Session Fragments	InvestigationEventRef...	1	UAP.common.context...	investigation	ip.src, ip.dst, ipv6.src, i...
□	Refocus EQUALS Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Refocus !EQUALS Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Refocus Contains Drill in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Find Session Fragments in New Tab	InvestigationEventRef...	1	UAP.common.context...	investigation	ip.src, ip.dst, ipv6.src, i...
□	Apply !EQUALS Drill	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply Contains Drill	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillab...
□	Apply !EQUALS Drill in New Tab	InvestigationEventDril...	1	UAP.common.context...	investigation	nw-event-value-drillab...
☑	**[Search Carbon Black - filename]**	**CarbonBlackSearchF...**	**Cus...**	**UAP.common.contex...**	**investigation**	**filename**

4. Refresh and navigate to the Investigation view.

5. Go to an event that has filename meta.

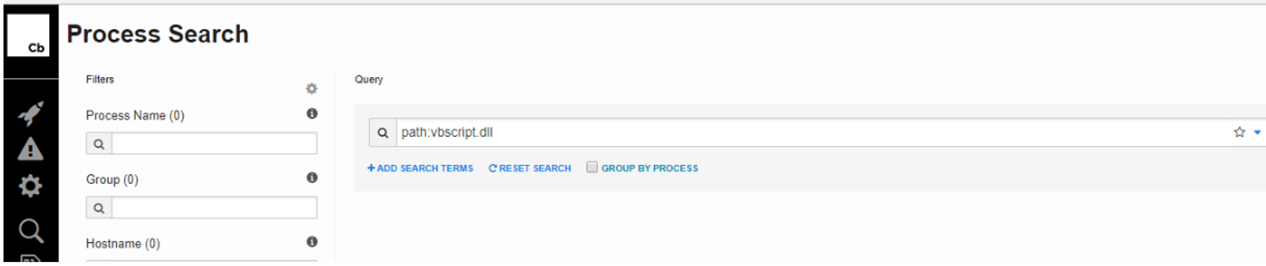
6. Right click on the filename, then choose **External Lookup > [Search Carbon Black - filename]** from the menu.



□	Event Time	Event Type	Event Theme	Size	Details
□	2017-10-18T12:18:46	Log	System.Unusual Activity	1 KB	device.class : Anti Virus header.id : 0005 event.time.str : 2017-10-18T16:10:05+05:30 product : CB version : 5.1 event.type : watchlist.storage.hit.binary event.vcat : Microsoft Corporation index : Microsoft ® VBScript obj.type : 5.8.9600.18817 group : Default Group index : 1 process : vbscript.dll reference.id : 0F1B16201BE1DF229182CE267FD4F4CE directory : c://windows//syswow64// filename : vbscript.dll extension : dll filename.size : 49 OS : Windows comp.version : 5.8 host.dst : localhos msg : cb_server=c ame=Microsoft Corporation copied_mod_len=499200 digsig_publisher=Microsoft Corporation digsig_result=Signed digsig_resul -15T01:02:00.000Z endpoint=244APP198|1 facet_id=572418 file_ msg.id : LEEF:01 msg.vid : LEEF event.cat : 16070 event.cat.name : did : nwappliance12192 rid : 19219

7. You are redirected to the Cb Response page.

> **Note:** You may need to log onto the Carbon Black website.



Note: You will need to repeat the procedure for the other available context menu actions (IP and hostname).

Add a Context Menu Action for IP Addresses

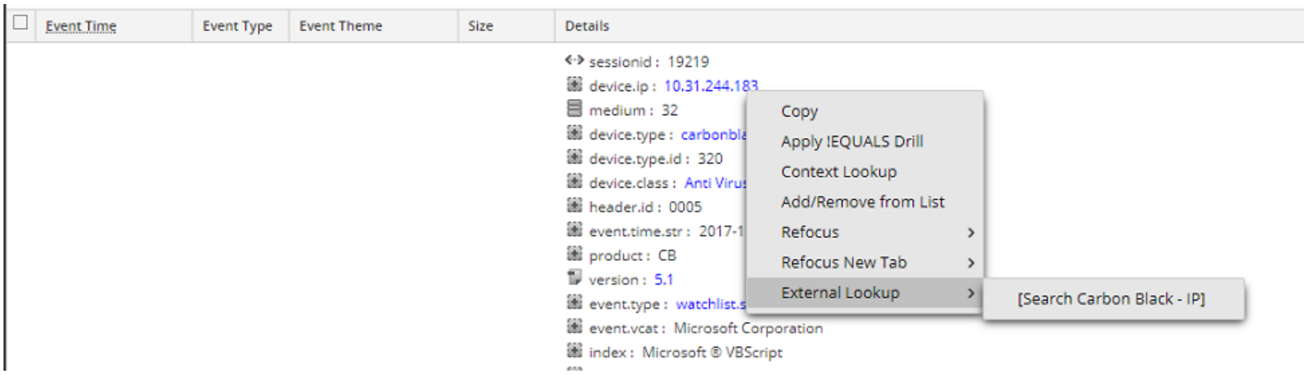
You should follow the basic procedure described in Add a Context Menu Action for Filename/Directory. The following actions are specific for adding the **device.ip** context menu action.

In step 3b, paste the following text into the Context Menu Configuration dialog box:

```
{

      "displayName": "[Search Carbon Black - filename]",
      "cssClasses": [
         "device.ip", "ip-dst",
         "ip.src", "ip.dst",
         "ipv6-src", "ipv6-dst",
         "ipv6.src", "ipv6.dst",
         "orig_ip",
      ],

      "description": "Carbon Black search IP",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "https://<Cb Server IP>/#/search?q=ipaddr%3A{0}",
      "disabled": "",
      "id": "CarbonBlackSearchIP",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true",
      "order":"16"

}
```

And just as you did in the previous procedure, replace ***<Cb Server IP>*** with the IP address of your Carbon Black server.

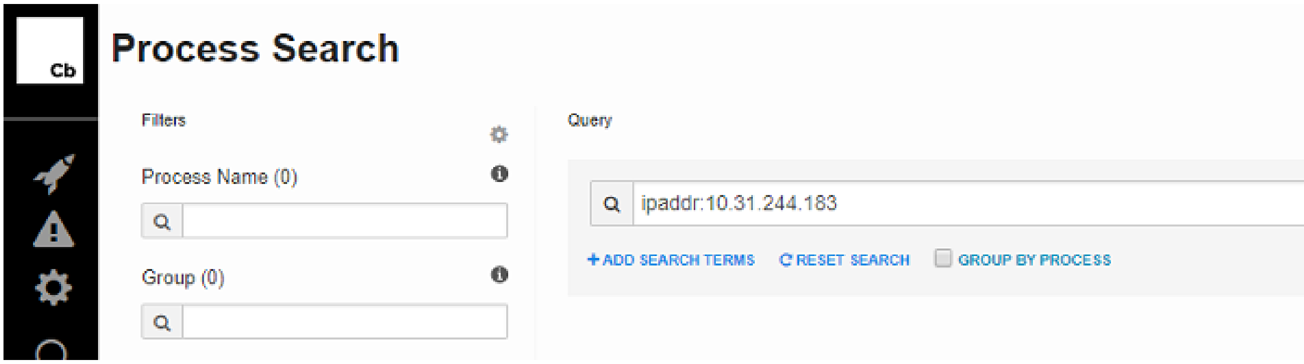
In the Investigation screen, navigate to an event that has device.ip meta, and right-click on the device.ip in the Details column. Then choose **External Lookup** > **[Search Carbon Black - IP]** from the menu:



□	Event Time	Event Type	Event Theme	Size	Details

sessionid : 19219
device.ip : 10.31.244.183
medium : 32
device.type : carbonbla
device.type.id : 320
device.class : Anti Virus
header.id : 0005
event.time.str : 2017-1
product : CB
version : 5.1
event.type : watchlist.s
event.vcat : Microsoft Corporation
index : Microsoft ® VBScript

You are redirected to the Cb Response page:



ipaddr:10.31.244.183

Add a Context Menu Action for Hostname

You should follow the basic procedure described in Add a Context Menu Action for Filename/Directory. The following actions are specific for adding the **Hostname** context menu action.

In step 3b, paste the following text into the Context Menu Configuration dialog box:

```
{

      "displayName": "[Search Carbon Black - hostname]",
      "cssClasses": [
         "alias-host",
         "alias.host",
         "host.src",
         "hostname",
      ],

      "description": "Carbon Black search hostname",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
      "version": "Custom",
      "modules": [
         "investigation"
      ],

      "local": "false",
      "groupName": "externalLookupGroup",
      "urlFormat": "https://<Cb Server IP>/#/search?q=hostname%3A{0}",
      "disabled": "",
      "id": "CarbonBlackSearchHostname",
      "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel",
         "UAP.investigation.events.view.EventGrid"
      ],
      "openInNewTab": "true",
      "order":"16"

}
```

And just as you did in the previous procedure, replace ***<Cb Server IP>*** with the IP address of your Carbon Black server.

In the Investigation screen, navigate to an event that has hostname meta, and right-click on the value in the Details column. Then choose **External Lookup > [Search Carbon Black - hostname]** from the menu.

You are redirected to the Cb Response page.

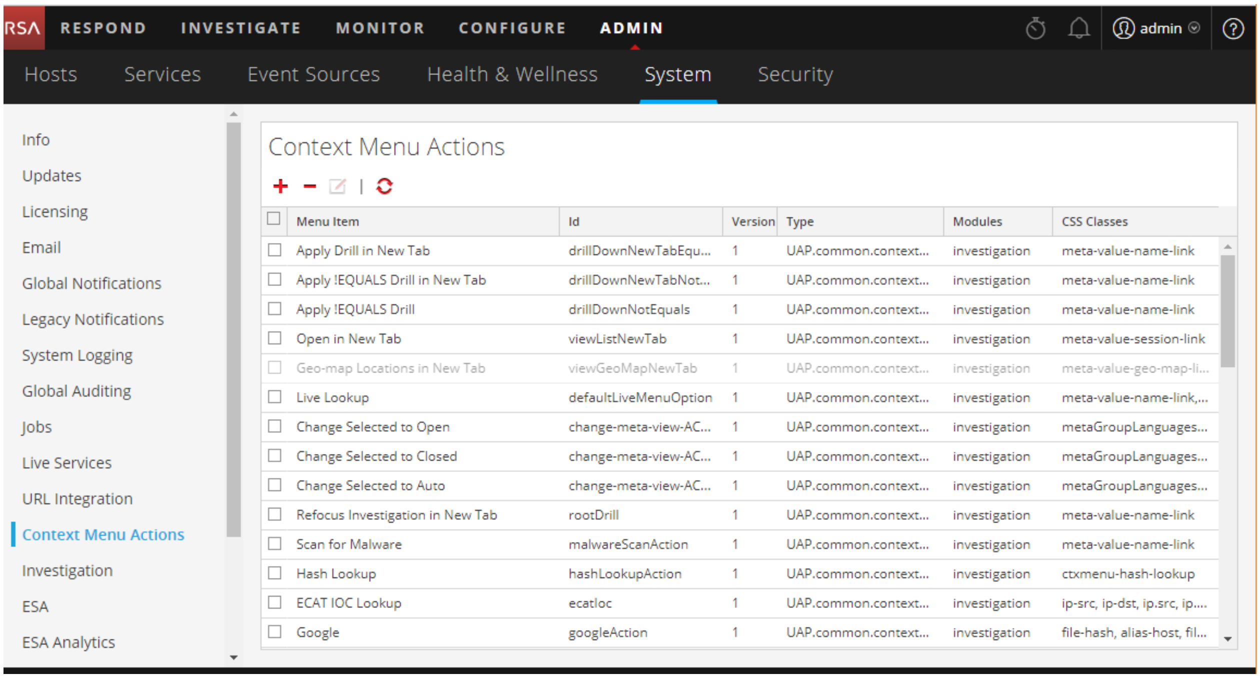
RSA NetWitness Investigation to Cb Live Response

Instead of pivoting from RSA NetWitness Investigation into the Carbon Black Response UI, analysts can pivot from Investigation into the Cb Live Response view.

To open the Cb Live Response window from the RSA NetWitness Investigator view:

1. Log onto the RSA NetWitness Platform UI.
2. Go to **ADMIN** > **System** > **Context Menu Actions**.

   The Context Menu Actions screen appears.



Context Menu Actions

☐	Menu Item	Id	Version	Type	Modules	CSS Classes
☐	Apply Drill in New Tab	drillDownNewTabEqu...	1	UAP.common.context...	investigation	meta-value-name-link
☐	Apply !EQUALS Drill in New Tab	drillDownNewTabNot...	1	UAP.common.context...	investigation	meta-value-name-link
☐	Apply !EQUALS Drill	drillDownNotEquals	1	UAP.common.context...	investigation	meta-value-name-link
☐	Open in New Tab	viewListNewTab	1	UAP.common.context...	investigation	meta-value-session-link
☐	Geo-map Locations in New Tab	viewGeoMapNewTab	1	UAP.common.context...	investigation	meta-value-geo-map-li...
☐	Live Lookup	defaultLiveMenuOption	1	UAP.common.context...	investigation	meta-value-name-link,...
☐	Change Selected to Open	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
☐	Change Selected to Closed	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
☐	Change Selected to Auto	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
☐	Refocus Investigation in New Tab	rootDrill	1	UAP.common.context...	investigation	meta-value-name-link
☐	Scan for Malware	malwareScanAction	1	UAP.common.context...	investigation	meta-value-name-link
☐	Hash Lookup	hashLookupAction	1	UAP.common.context...	investigation	ctxmenu-hash-lookup
☐	ECAT IOC Lookup	ecatloc	1	UAP.common.context...	investigation	ip-src, ip-dst, ip.src, ip....
☐	Google	googleAction	1	UAP.common.context...	investigation	file-hash, alias-host, fil...

3. Add the Carbon Black Live Context Menu Action.

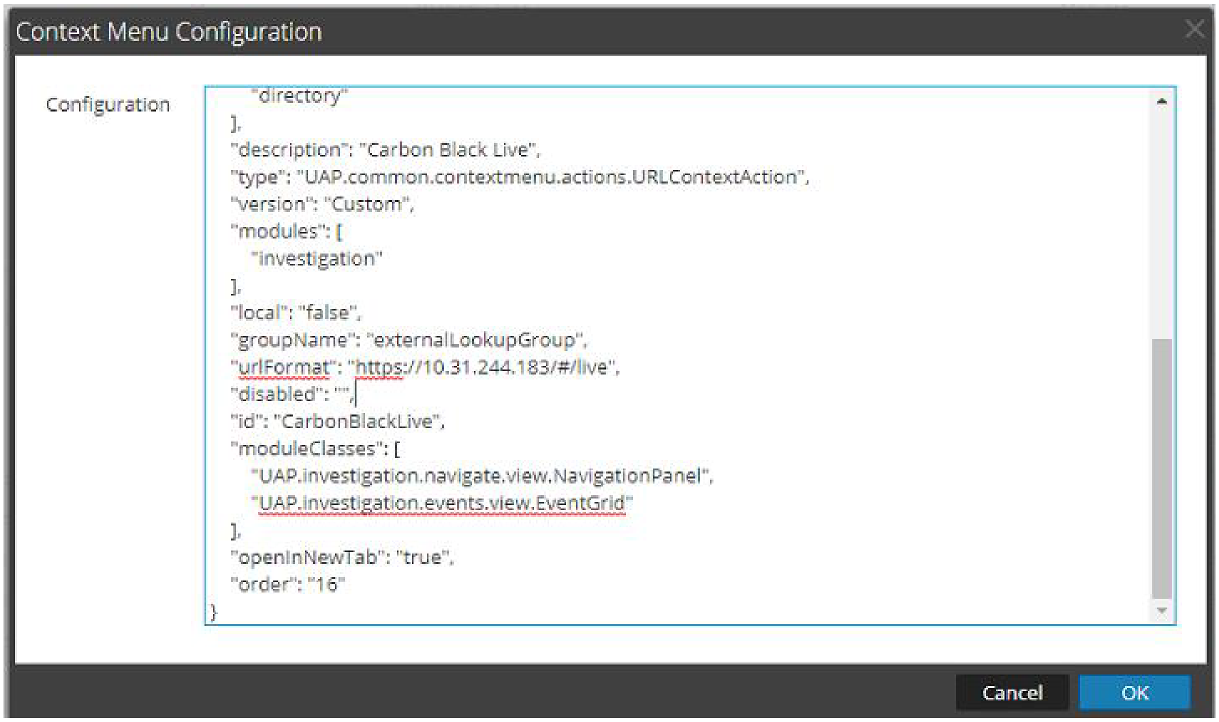
   a. In the toolbar, click +.

      The Context Menu Configuration dialog box appears.

   b. Paste the following text into the Context Menu Configuration dialog box :

```
{

      "displayName": "[Search Carbon Black Live]",
      "cssClasses": [
         "alias-host",
         "alias.host",
         "device.ip",
         "ip-dst",
         "ip.src",
         "ip.dst",
        "ipv6-src",
        "ipv6-dst",
        "ipv6.src",
        "ipv6.dst",
        "orig_ip",
        “hostname”,
        “host.src”,
        "filename",
        "directory"

   ],

   "description": "Carbon Black Live",
   "type": "UAP.common.contextmenu.actions.URLContextAction",
   "version": "Custom",
   "modules": [
        "investigation"
   ],

   "local": "false",
   "groupName": "externalLookupGroup",
   "urlFormat": "https://<Cb Server IP>/#/live",
   "disabled": "",
   "id": "CarbonBlackLive",
   "moduleClasses": [
        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
   ],
   "openInNewTab": "true",
   "order":"16"

}
```

The screen should look similar to this:



```
    "directory"
  ],
  "description": "Carbon Black Live",
  "type": "UAP.common.contextmenu.actions.URLContextAction",
  "version": "Custom",
  "modules": [
    "investigation"
  ],
  "local": "false",
  "groupName": "externalLookupGroup",
  "urlFormat": "https://10.31.244.183/#/live",
  "disabled": "",
  "id": "CarbonBlackLive",
  "moduleClasses": [
    "UAP.investigation.navigate.view.NavigationPanel",
    "UAP.investigation.events.view.EventGrid"
  ],
  "openInNewTab": "true",
  "order": "16"
}
```

c. Replace **<Cb Server IP>** with the IP address of your Carbon Black server. for example, in the above image, the line is as follows:

```
"urlFormat": "https://10.31.244.183/#/live",
```

Note: If you are not using SSL, change **https** to **http**.

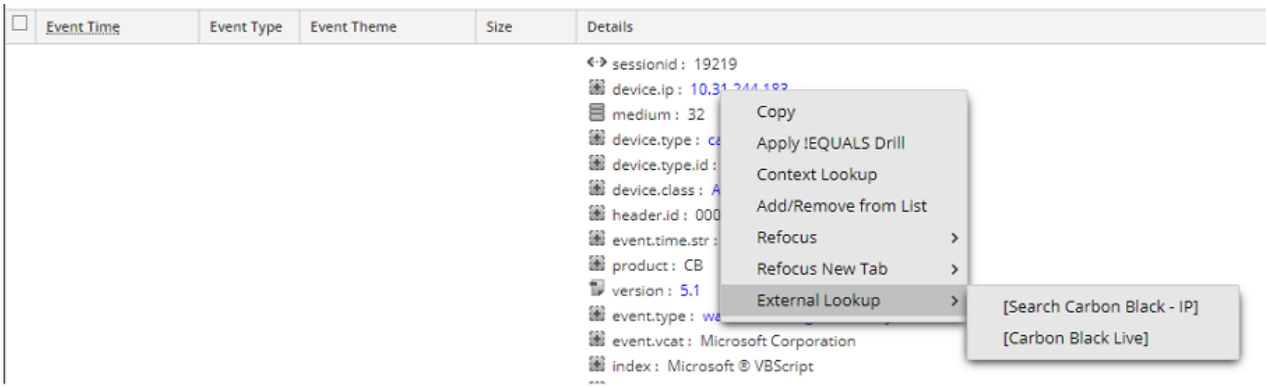
d. Click OK.

The context menu action is added to the end of the list.

4. Refresh and navigate to the Investigation view.

5. Go to an event that has any of the meta values listed in the context menu configuration code (for example **alias.host**, **device.ip**, **filename** and so on).

6. Right click on the filename, then choose **External Lookup > [Search Carbon Black Live]** from the menu.

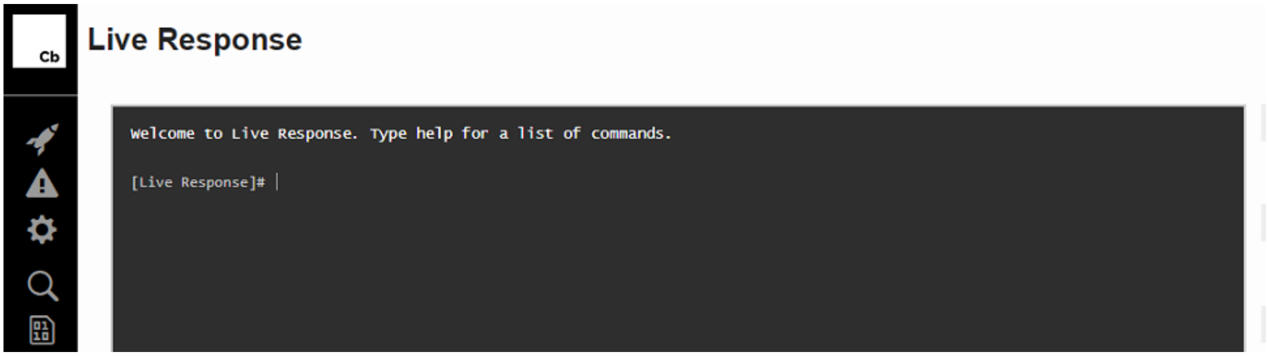


☐	Event Time	Event Type	Event Theme	Size	Details

```
sessionid : 19219
device.ip : 10.31.244.183
medium : 32
device.type : ca
device.type.id :
device.class : A
header.id : 000
event.time.str :
product : CB
version : 5.1
event.type : wa
event.vcat : Microsoft Corporation
index : Microsoft ® VBScript
```

7. You are redirected to the Cb Live Response page.

Note: You may need to log onto the Carbon Black website.



```
Welcome to Live Response. Type help for a list of commands.

[Live Response]# |
```

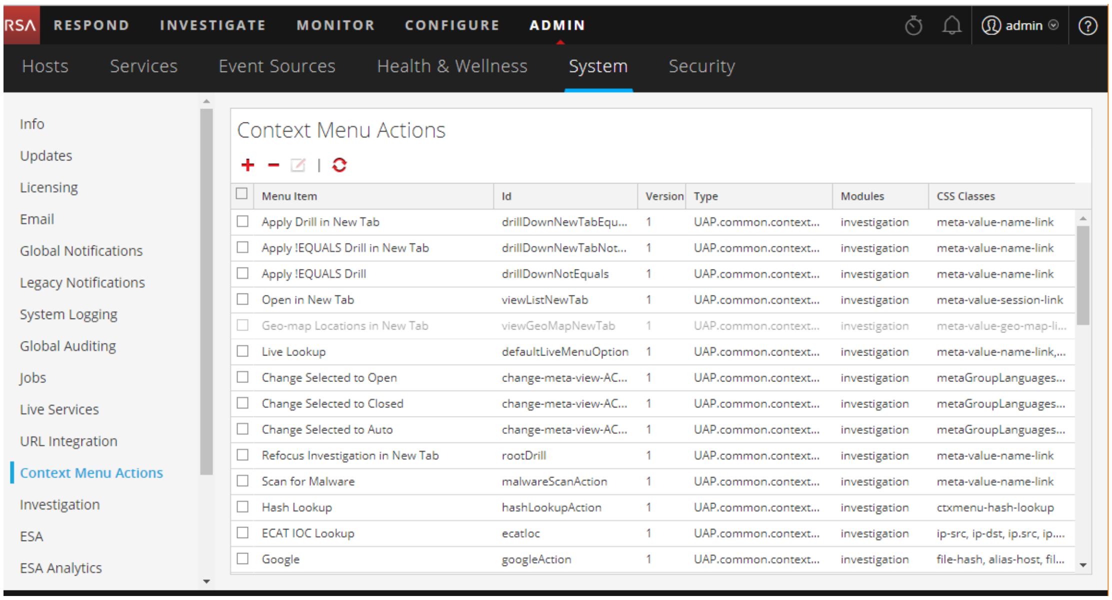
RSA NetWitness Investigation to Cb Response Isolate Host

Isolation of Host is a detailed step process in Cb Response. The best place to search for the same is on the 'Process Search' screen. Clicking on any process shown in the Search page of the Cb UI directs you to a detailed view page, where you can isolate the Host.

To open the Isolate Host window from the RSA NetWitness Investigator view:

1. Log onto the RSA NetWitness Platform UI.
2. Go to **ADMIN** > **System** > **Context Menu Actions**.

   The Context Menu Actions screen appears.



Context Menu Actions

□	Menu Item	Id	Version	Type	Modules	CSS Classes
□	Apply Drill in New Tab	drillDownNewTabEqu...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill in New Tab	drillDownNewTabNot...	1	UAP.common.context...	investigation	meta-value-name-link
□	Apply !EQUALS Drill	drillDownNotEquals	1	UAP.common.context...	investigation	meta-value-name-link
□	Open in New Tab	viewListNewTab	1	UAP.common.context...	investigation	meta-value-session-link
□	Geo-map Locations in New Tab	viewGeoMapNewTab	1	UAP.common.context...	investigation	meta-value-geo-map-li...
□	Live Lookup	defaultLiveMenuOption	1	UAP.common.context...	investigation	meta-value-name-link,...
□	Change Selected to Open	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Closed	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Change Selected to Auto	change-meta-view-AC...	1	UAP.common.context...	investigation	metaGroupLanguages...
□	Refocus Investigation in New Tab	rootDrill	1	UAP.common.context...	investigation	meta-value-name-link
□	Scan for Malware	malwareScanAction	1	UAP.common.context...	investigation	meta-value-name-link
□	Hash Lookup	hashLookupAction	1	UAP.common.context...	investigation	ctxmenu-hash-lookup
□	ECAT IOC Lookup	ecatioc	1	UAP.common.context...	investigation	ip-src, ip-dst, ip.src, ip....
□	Google	googleAction	1	UAP.common.context...	investigation	file-hash, alias-host, fil...

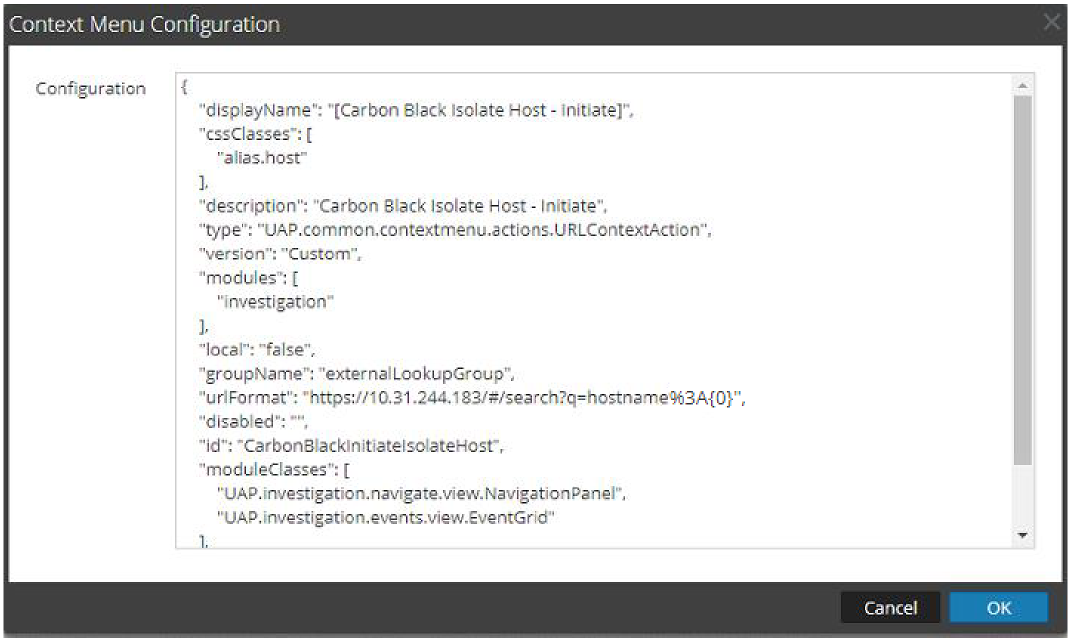
3. Add the Carbon Black Host Initiate Context Menu Action.
   a. In the toolbar, click +.

      The Context Menu Configuration dialog box appears.

   b. Paste the following text into the Context Menu Configuration dialog box :

```
{

      "displayName": "[Carbon Black Isolate Host - Initiate]",
      "cssClasses": [
         "alias.host",

      ],

      "description": "Carbon Black Isolate Host - Initiate",
      "type": "UAP.common.contextmenu.actions.URLContextAction",
        "version": "Custom",
        "modules": [
           "investigation"
        ],

        "local": "false",
        "groupName": "externalLookupGroup",
        "urlFormat": "https://<Cb Server IP>/#/search?q=hostname%3A{0}",
        "disabled": "",
        "id": "CarbonBlackInitiateIsolateHost",
        "moduleClasses": [
           "UAP.investigation.navigate.view.NavigationPanel",
           "UAP.investigation.events.view.EventGrid"
        ],
        "openInNewTab": "true",
        "order":"16"

}
```

The screen should look similar to this:



```
{
   "displayName": "[Carbon Black Isolate Host - Initiate]",
   "cssClasses": [
      "alias.host"
   ],
   "description": "Carbon Black Isolate Host - Initiate",
   "type": "UAP.common.contextmenu.actions.URLContextAction",
   "version": "Custom",
   "modules": [
      "investigation"
   ],
   "local": "false",
   "groupName": "externalLookupGroup",
   "urlFormat": "https://10.31.244.183/#/search?q=hostname%3A{0}",
   "disabled": "",
   "id": "CarbonBlackInitiateIsolateHost",
   "moduleClasses": [
      "UAP.investigation.navigate.view.NavigationPanel",
      "UAP.investigation.events.view.EventGrid"
   ],
```

c. Replace **<Cb Server IP>** with the IP address of your Carbon Black server. for example, in the above image, the line is as follows:

```
"urlFormat": "https://10.31.244.183/#/search?q=hostname%3A{0",
```

> **Note:** If you are not using SSL, change **https** to **http**.

d. Click OK.

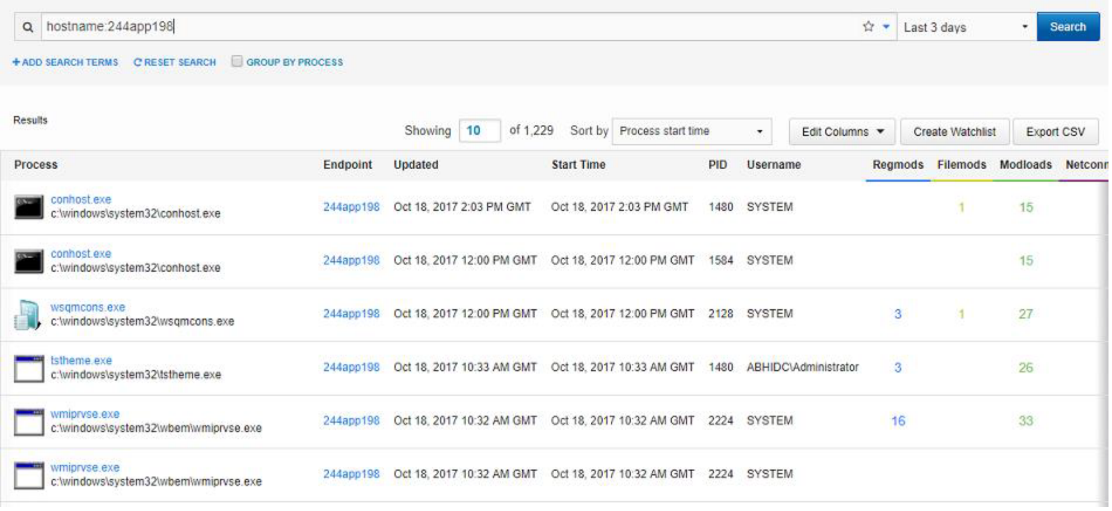
The context menu action is added to the end of the list.

4. Refresh and navigate to the Investigation view.

5. Go to an event that has a hostname (alias.host) meta value.
6. Right click on the hostname, then choose **External Lookup > [Carbon Black Isolate Host - Initiate]** from the menu.
7. You are redirected to the Cb Response Process Search page for hostname.

   Note: You may need to log onto the Carbon Black website.

8. Click **Search**.



hostname:244app198

Last 3 days

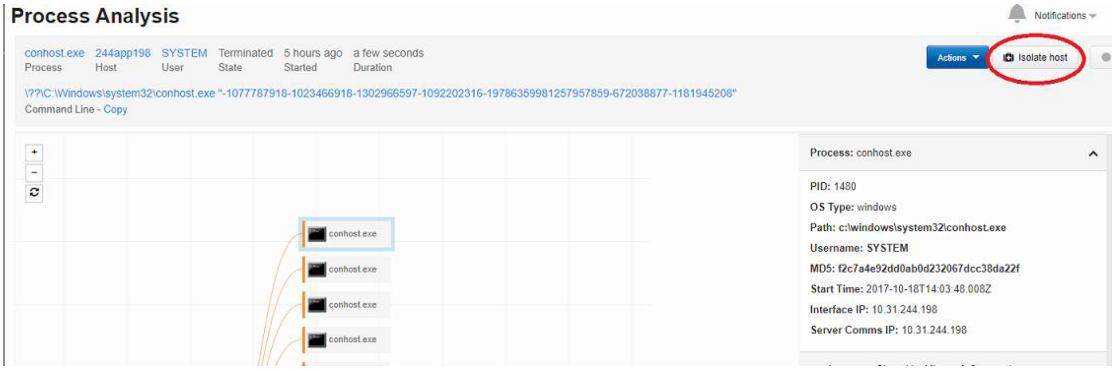
Results

Showing 10 of 1,229 Sort by Process start time

Process	Endpoint	Updated	Start Time	PID	Username	Regmods	Filemods	Modloads	Netconn
conhost.exe c:\windows\system32\conhost.exe	244app198	Oct 18, 2017 2:03 PM GMT	Oct 18, 2017 2:03 PM GMT	1480	SYSTEM		1	15	
conhost.exe c:\windows\system32\conhost.exe	244app198	Oct 18, 2017 12:00 PM GMT	Oct 18, 2017 12:00 PM GMT	1584	SYSTEM			15	
wsqmcons.exe c:\windows\system32\wsqmcons.exe	244app198	Oct 18, 2017 12:00 PM GMT	Oct 18, 2017 12:00 PM GMT	2128	SYSTEM	3	1	27	
tstheme.exe c:\windows\system32\tstheme.exe	244app198	Oct 18, 2017 10:33 AM GMT	Oct 18, 2017 10:33 AM GMT	1480	ABHIDC\Administrator	3		26	
wmiprvse.exe c:\windows\system32\wbem\wmiprvse.exe	244app198	Oct 18, 2017 10:32 AM GMT	Oct 18, 2017 10:32 AM GMT	2224	SYSTEM	16		33	
wmiprvse.exe c:\windows\system32\wbem\wmiprvse.exe	244app198	Oct 18, 2017 10:32 AM GMT	Oct 18, 2017 10:32 AM GMT	2224	SYSTEM				

9. Click the process on which to perform your search.

   You can Isolate the Host (from the **Actions** menu), or carry on with the analysis.



Process Analysis

conhost.exe	244app198	SYSTEM	Terminated	5 hours ago	a few seconds
Process	Host	User	State	Started	Duration

\??\C:\Windows\system32\conhost.exe "-1077787918-1023466918-1302966597-1092202316-19786359981257957859-672038877-1181945208"
Command Line - Copy

Process: conhost.exe

PID: 1480
OS Type: windows
Path: c:\windows\system32\conhost.exe
Username: SYSTEM
MD5: f2c7a4e92dd0ab0d232067dcc38da22f
Start Time: 2017-10-18T14:03:48.008Z
Interface IP: 10.31.244.198
Server Comms IP: 10.31.244.198

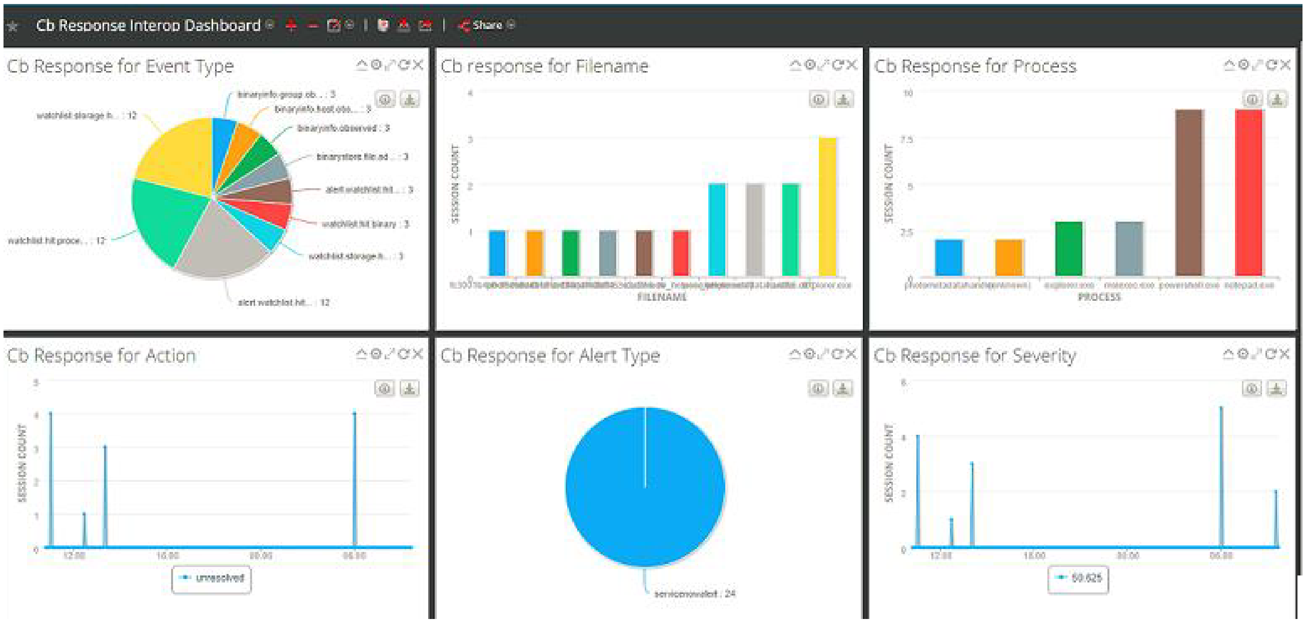
Cb Response File Delete

You can use the Cb Live Response window to delete files through the command line interface. In the RSA NetWitness Investigation view, right click a filename meta value and click **External Lookup > [Carbon Black Live]** from the menu.

From here, you can run the commands necessary to delete a specified file. For details, see the Carbon Black documentation.

Cb Response Interop Dashboard

The data from Cb Response can be used to create a Dashboard in the RSA NetWitness UI for easy monitoring. Below is a screenshot showing the **Cb Response Interop Dashboard**.



Dashlets Contained in this Dashboard

The **Cb Response Interop Dashboard** dashboard contains the following dashlets:

- **Cb Response by Event Type** (event.type)
- **Cb Response by details for Filename** (filename)
- **Cb Response for Process** (process)
- **Cb Response by Action** (action)
- **Cb Response on Alert Type** (alert)
- **Cb Response by Severity** (severity)

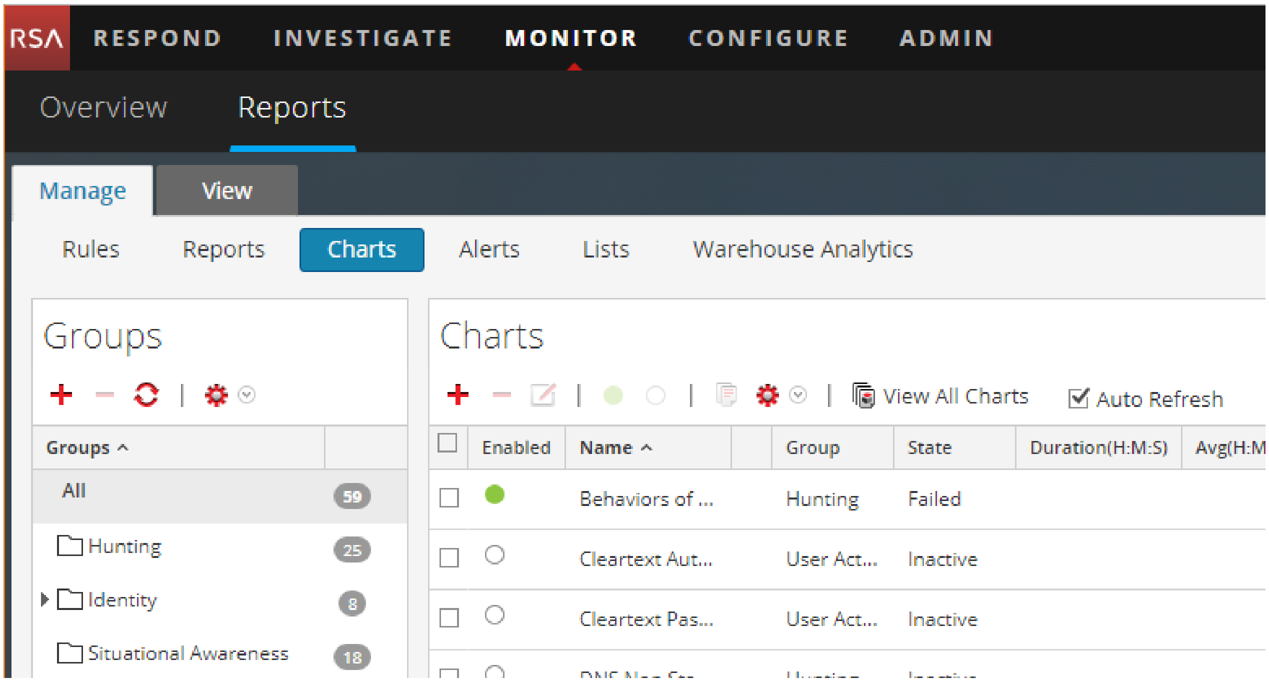
Import the Charts

1. Download the dashboard files and save them to your file system.

   There is a ZIP archive and a configuration file:

- **Cb Response Interop.zip**
- **Cb+Response+Interop.cfg**

2. Log on to the RSA NetWitness UI and, go to **MONITOR** > **Reports**.
3. Select **Charts** from the Manage tab.



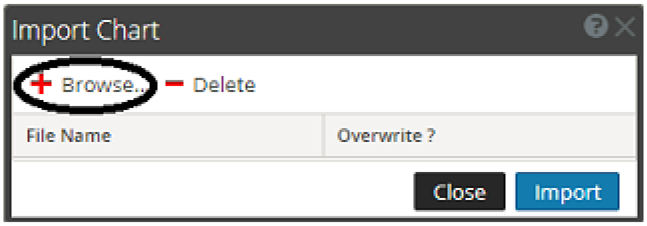
Groups ^	
All	59
Hunting	25
Identity	8
Situational Awareness	18

□	Enabled	Name ^	Group	State	Duration(H:M:S)	Avg(H:M
□	●	Behaviors of ...	Hunting	Failed		
□	○	Cleartext Aut...	User Act...	Inactive		
□	○	Cleartext Pas...	User Act...	Inactive		

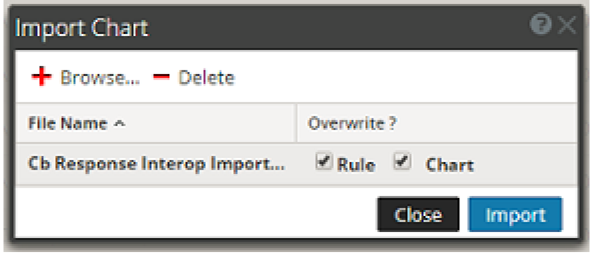
4. From the **Groups** pane, click ⚙ > **Import**.

   The Import Chart dialog box displays.

5. Click Browse and navigate to the folder where you saved the **Cb Response Interop.zip** file.



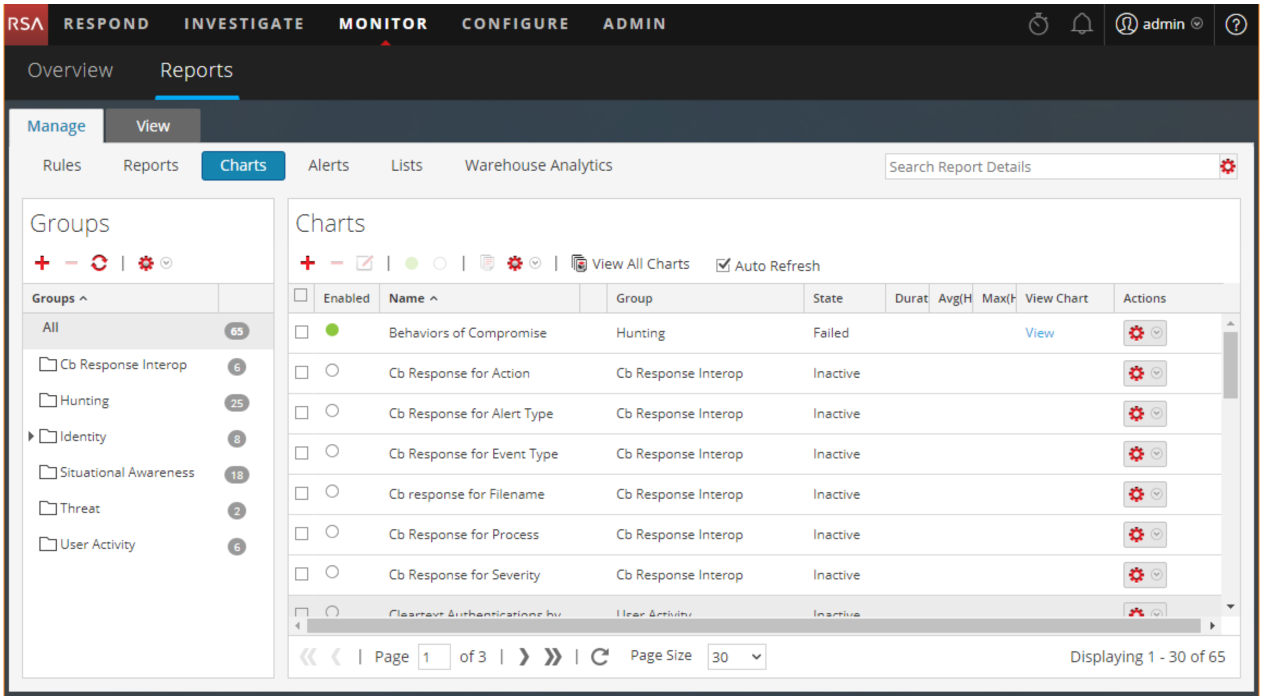
6. Select both the **Rule** and **Chart** fields.



File Name ^	Overwrite ?
Cb Response Interop Import...	☑ Rule ☑ Chart

7. Click **Import**.

   The new charts appears in the list in the Charts pane.



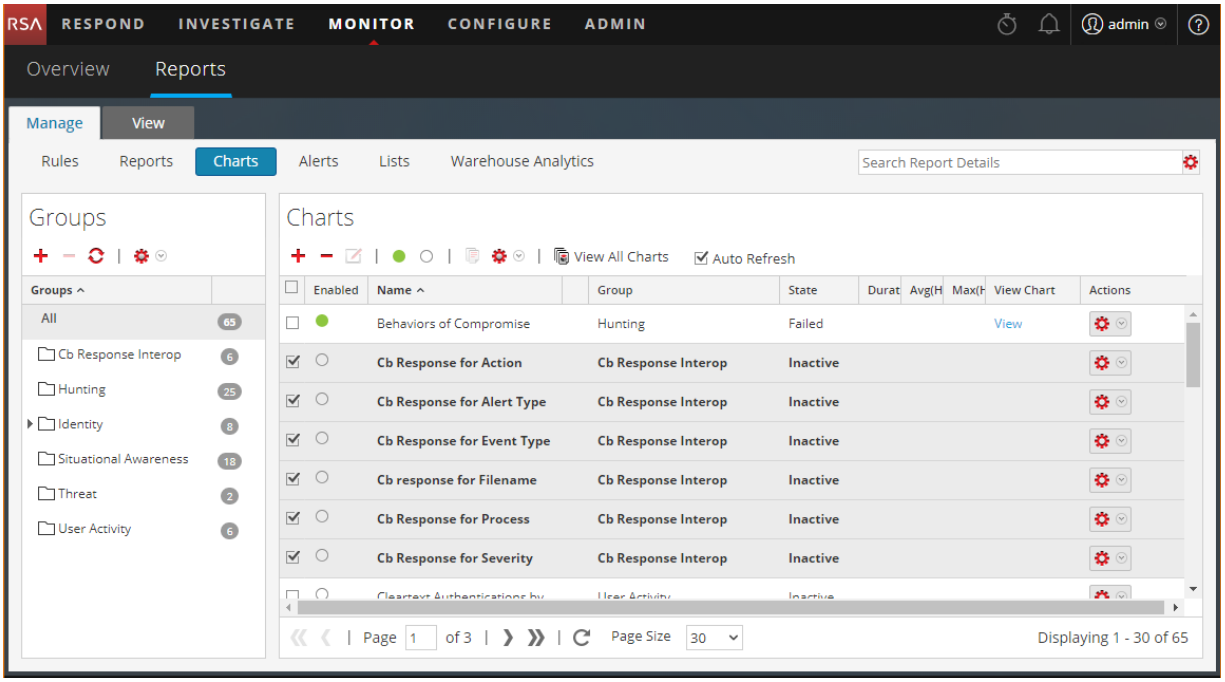
Groups ^	
All	65
Cb Response Interop	6
Hunting	25
Identity	8
Situational Awareness	18
Threat	2
User Activity	6

□	Enabled	Name ^	Group	State	Durat	Avg(H	Max(H	View Chart	Actions
□	●	Behaviors of Compromise	Hunting	Failed				View	
□	○	Cb Response for Action	Cb Response Interop	Inactive					
□	○	Cb Response for Alert Type	Cb Response Interop	Inactive					
□	○	Cb Response for Event Type	Cb Response Interop	Inactive					
□	○	Cb response for Filename	Cb Response Interop	Inactive					
□	○	Cb Response for Process	Cb Response Interop	Inactive					
□	○	Cb Response for Severity	Cb Response Interop	Inactive					
□	○	Cleartext Authentications by	User Activity	Inactive					

Note: The newly imported charts are disabled.

8. To enable the charts:

a. Select the Cb Response charts:



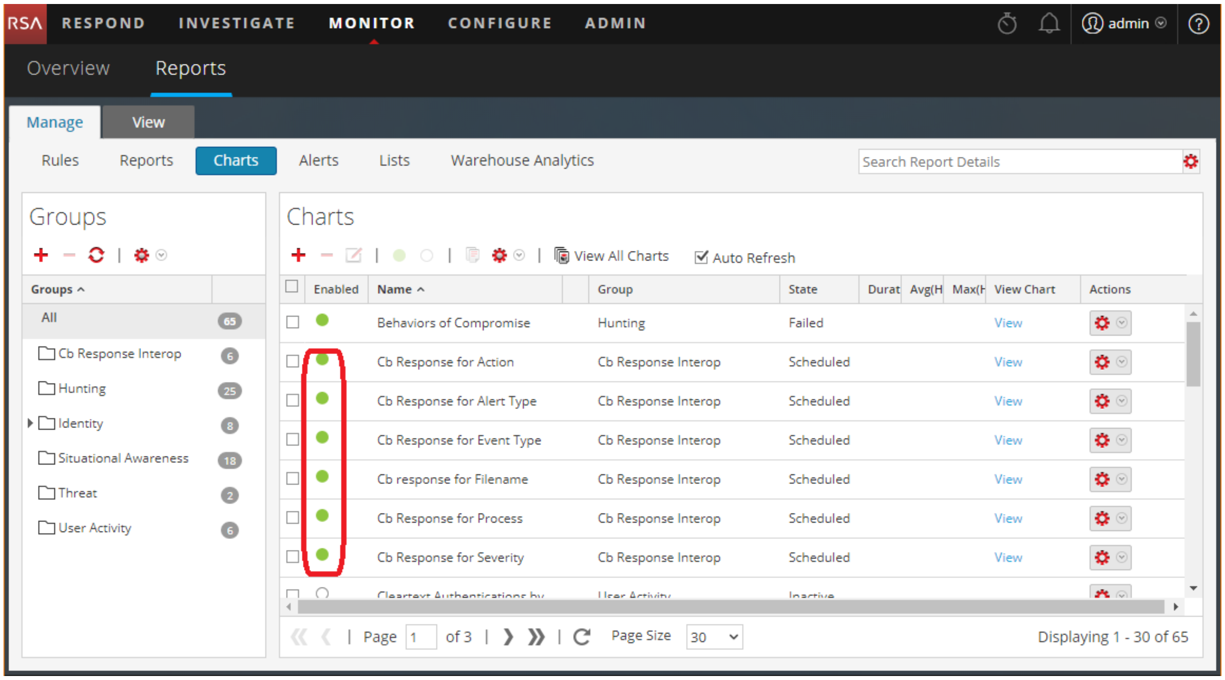
Groups ^	
All	65
Cb Response Interop	6
Hunting	25
Identity	8
Situational Awareness	18
Threat	2
User Activity	6

☐	Enabled	Name ^	Group	State	Durat	Avg(H	Max(H	View Chart	Actions
☐	●	Behaviors of Compromise	Hunting	Failed				View	
☑	○	**Cb Response for Action**	**Cb Response Interop**	**Inactive**					
☑	○	**Cb Response for Alert Type**	**Cb Response Interop**	**Inactive**					
☑	○	**Cb Response for Event Type**	**Cb Response Interop**	**Inactive**					
☑	○	**Cb response for Filename**	**Cb Response Interop**	**Inactive**					
☑	○	**Cb Response for Process**	**Cb Response Interop**	**Inactive**					
☑	○	**Cb Response for Severity**	**Cb Response Interop**	**Inactive**					
☐	○	Cleartext Authentications by	User Activity	Inactive					

Page 1 of 3 | Page Size 30 | Displaying 1 - 30 of 65

b. Click the round, green icon (●) to enable the charts.

The icon for each chart changes to green to indicate the charts are enabled.



Groups ^	
All	65
Cb Response Interop	6
Hunting	25
Identity	8
Situational Awareness	18
Threat	2
User Activity	6

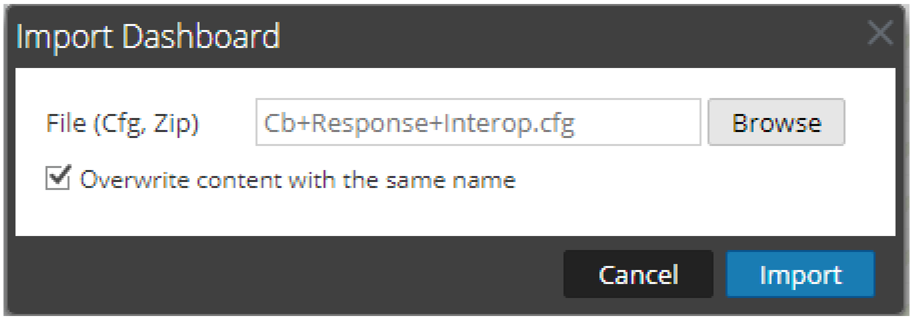
☐	Enabled	Name ^	Group	State	Durat	Avg(H	Max(H	View Chart	Actions
☐	●	Behaviors of Compromise	Hunting	Failed				View	
☐	●	Cb Response for Action	Cb Response Interop	Scheduled				View	
☐	●	Cb Response for Alert Type	Cb Response Interop	Scheduled				View	
☐	●	Cb Response for Event Type	Cb Response Interop	Scheduled				View	
☐	●	Cb response for Filename	Cb Response Interop	Scheduled				View	
☐	●	Cb Response for Process	Cb Response Interop	Scheduled				View	
☐	●	Cb Response for Severity	Cb Response Interop	Scheduled				View	
☐	○	Cleartext Authentications by	User Activity	Inactive					

Page 1 of 3 | Page Size 30 | Displaying 1 - 30 of 65

Add the Dashboard

1. Depending on your version:
   - In RSA NetWitness 11.x, go to **MONITOR > Overview**
   - In RSA Security Analytics 10.x, from the Security Analytics menu, select **Dashboard**.
2. Click the Import Dashboard button () from the menu bar.

   The Import Dashboard dialog box is displayed.
3. Click Browse and navigate to the folder where you saved the **Cb+Response+Interop.cfg** file.



File (Cfg, Zip) Cb+Response+Interop.cfg

☑ Overwrite content with the same name

4. Click **Import**.

The dashboard appears in the UI.

CbAPI Response Feeds

RSA NetWitness can use the CbResponse 6.0 API (Python Version) to connect to the Carbon Black Feed system and extract the feed data from the same. After extracting the data for IPv4, MD5 and DNS, RSA NetWitness would utilize them by adding them as a feed into the RSA NetWitness system. This allows an analyst to use the Threat Intelligence Capabilities of Carbon Black with RSA NetWitness in one place, to help make a more informed security decision.

Prerequisites

The following items are need before you can create CbAPI response feeds in RSA NetWitness.

- **Identification of a machine**

  For creation of recurring feeds on RSA NetWitness, a URL is needed for the csv file from which the feeds should be created. Therefore, a machine with WebService running is essential. Also, the same machine should be reachable from the UI and be able to communicate with the Carbon Black device.

  You can use the RSA NetWitness head unit for this purpose. If so, add the files into the `/var/netwitness/srv/www` folder, using an SSH tool (such as WinSCP).

- **A minimal version of Python**

  For the included script to work correctly, RSA recommends Python 3.3 or newer on the machine that is going to run the script.

Configure RSA NetWitness for CbAPI Response

You need to set up Python so that the necessary version and packages exist on the RSA NetWitness Log Decoder.

1. SSH into the RSA NetWitness Log Decoder with Administrative Credentials.
2. Determine your version of Python by running the following command:

   ```
   python --version
   ```

   If the version is less than 2.7.6, you need to install Python 3.3.

- If you are running RSA NetWitness 11.0, check for Python 3.3.
- If you are running RSA Security Analytics 10.6.x, download and install Python 3.3.x.

3. Run the following command:

   ```
   source /opt/rh/python33/enable
   ```

4. Run the following command:

   ```
   pip3.3 install cbapi
   ```

   Note: If **pip3.3** is not present, use Python **easy_install** to install it, then rerun the above command.

5. Next, run:

   ```
   cbapi-response configure
   ```

   Follow the steps in the Carbon Black Rest API Quick Start guide (currently located here, but be aware the URL could change: https://developer.carbonblack.com/guide/enterprise-response/cbrestapiquickstart/).

6. Make sure the following packages exist:

   - In `/opt/rh/python33/root/usr/lib/python3.3/site-packages/`, make sure **cbapi** exists
   - In `/opt/rh/python33/root/usr/lib/python3.3/site-packages/cbapi/`, make sure **response** exists.

Download and Install Feed Files

RSA provides the necessary files that you need for using the CbAPI Response feeds in RSA NetWitness.

To download and install the feed files:

1. Download **Carbon Black_RSA NetWitness.zip** from RSA Link here: Carbon Black Cb Response - RSA NetWitness Parser Source Package.
2. Unpack the Zip archive and make sure you see the following files:
   - CbFeeds.py
   - cbfeed.ini
3. SSH into the RSA NetWitness SA Head with Administrative Credentials.
4. Create a folder to hold the feed files by running the following command:

   ```
   mkdir cbfeed
   ```

   Note: The cbfeed directory is used by the CRON job. So, if you change the name, make sure to use the same path name when you create and configure the CRON job.

5. Copy the supplied files into the **/cbfeed** folder that you just created.

To verify the feeds are installed and working correctly:

1. Update the configuration file, **cbfeed.ini**, as described in the following table.

   Note: The CbFeed.py script looks for the **cbfeed.ini** file first in the directory from where the script is being run. So, make sure the .ini file is in the same folder as the .py file.

Parameter	Description
PATH	Specify the path where you want the .csv files to be copied to the webserver. If it is for the RSA NetWitness SA Head, use the default value, `/var/netwitness/srv/www/`.
ARCHIVE	This is a Boolean value, either TRUE or FALSE. The default value is FALSE. Set the value to TRUE to archive the .csv files that get created every time the script runs. If TRUE, the script will create an **/archive** folder. In that folder, every run adds new files by appending the name with the UTC timestamp. So, for example, a **cbfeeddns.csv** file would be copied to **/archive** folder with the name **cbfeeddns_*<UTC-Time-Stamp>*.csv**. RSA recommends keeping this value FALSE, unless an archive is essential, as a value of TRUE could use a lot of disk space.
SOURCE	Specify the directory where you want to create the .csv files. This directory would also contain the **/archive** sub-folder if you have set ARCHIVE to TRUE. RSA recommends that you set the value of this parameter to the directory you created earlier, in Step 3.

2. Test whether the feed works. Run the following commands:

```
cd <directory structure>/cbfeed
source /opt/rh/python33/enable
python CbFeed.py
```

3. The program should execute without issues. Check the **/cbfeed** directory for the following new files:
   - cbfeeddns.csv
   - cbfeedmd5.csv
   - cbfeedipv4.csv

   Additionally, if you set ARCHIVE to true, you should see a sub-folder named **archive**.

4. If the above files exist, check `/var/netwitnesssrv/www/` for the following files:
   - cbfeeddns.csv
   - cbfeedmd5.csv
   - cbfeedipv4.csv

5. To check whether the webserver is working, perform the following steps:

   a. Open a browser.

   b. For the URL, enter **http://<*IP-of-the-webserver*>/cbfeeddns.csv**.

   The system should start downloading the .csv file.

Configure Cron Job for the Feed

Set up a cron job to update the feeds information at specified time intervals. You can set the cron job to run at various frequency, such as hourly, every 4 hours, and so on. In the following procedure, we set the frequency so the feed is updated every 4 hours.

1. Open a terminal and SSH to the Log Decoder box using Administrative credentials.
2. Run the following command:

   ```
   crontab -e
   ```

   This opens crontab in a vim editor.

3. Press ‘i’ to enter edit mode, and navigate to the final line in the file.
4. Copy the following line into the editor:

   ```
   * 0,4,8,12,16,20 * * * source /opt/rh/python33/enable && cd <directory-path>/cbfeed &&
   python CbFeed.py > /tmp/feed.log 2>&1
   ```

   Make sure to replace ***<directory-path>*** with the actual path to the cbfeed folder in your system.

5. Press the Escape key, then enter **:wq!** to save your work and close the vim editor.

   The following message is displayed, indicating that the job is installing correctly:

   ```
   crontab: installing new crontab
   ```

The job will run every 4 hours, and the details are logged to **/tmp/feed.log**.

Create the Recurring Feed in RSA NetWitness

1. Depending on your version:
   - For NetWitness 11.x: In the **RSA NetWitness** menu, select **CONFIGURE > Custom Feeds**.
   - For Security Analytics 10.x: In the **RSA Security Analytics** menu, select **Live > Feeds**.
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.

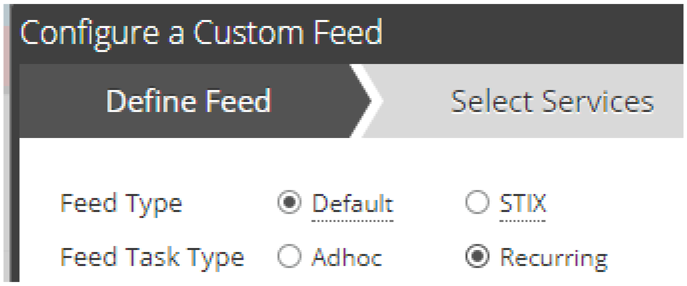
3. To select the feed type, click **Custom Feed** and **Next**.

The Configure a Custom Feed wizard is displayed, with the Define Feed form open.

4. Walk through the Custom Feed wizard.

   a. In the Define Feed form, select the following values:

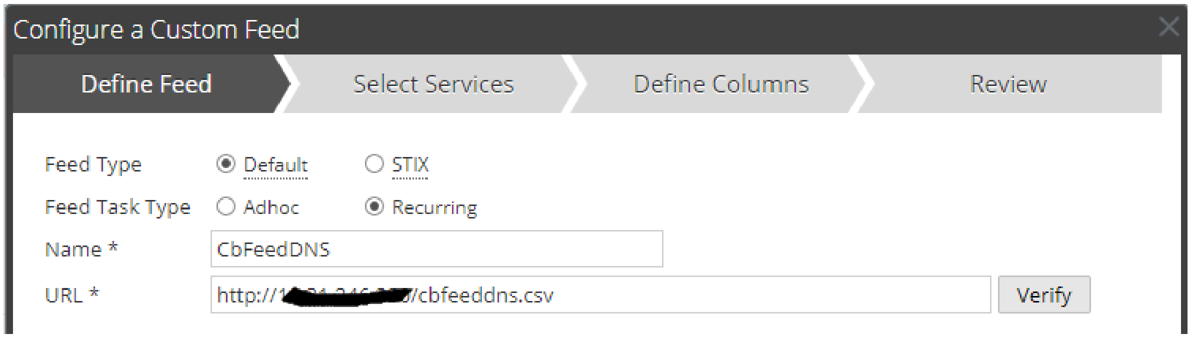
      - For **Feed Type**, choose one of the following, based on your version:
        - In RSA Security Analytics 10.x, select **Default**
        - In RSA NetWitness 11.x, select **CSV**
      - For **Feed task Type**, choose **Recurring**.



Feed Type ● Default ○ STIX

Feed Task Type ○ Adhoc ● Recurring

      - Enter one of the feeds in the Name field, for example **CBFeedDNS** for the DNS feed.
      - For the URL, enter **http://*<IP-of-the-webserver>*/cbfeeddns.csv**, where *<IP-of-the-webserver>* is the IP address your webserver.



Feed Type ● Default ○ STIX

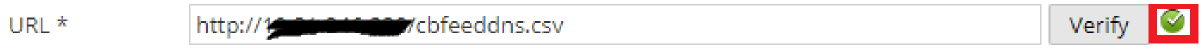
Feed Task Type ○ Adhoc ● Recurring

Name * CbFeedDNS

URL * http://[redacted]/cbfeeddns.csv

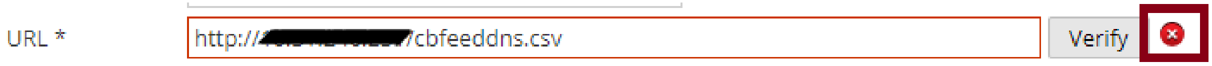
   b. Click **Verify**.

      If verification is successful, you will see ✓.



URL * http://[redacted]/cbfeeddns.csv

      If, rather, it fails, you will see ✗.

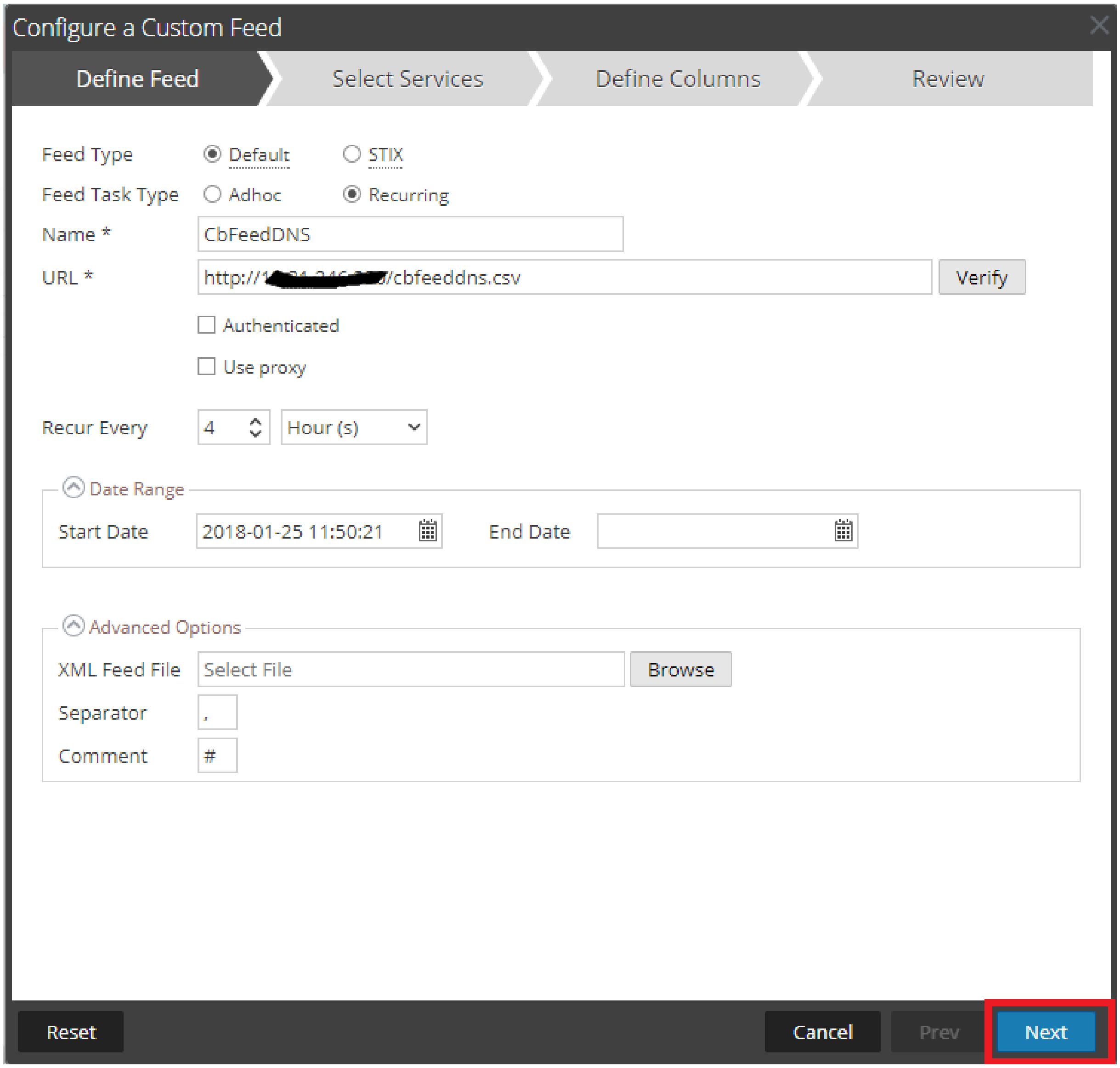


URL * http://[redacted]/cbfeeddns.csv

   c. If the verification fails, you can try typing the URL directly into a browser, and see if that works.

   d. For **Recur Every**, select a number, for example 4. In the drop-down menu, select a time range, for example **Hour(s)**, for a recurring feed that refreshes itself every 4 hours.

e. For the Date Range, the **Start Date** defaults to the current date and time. You can accept this value, or enter a future date. Leave the **End Date** empty if you do not want an end date.



Configure a Custom Feed

Feed Type ● Default ○ STIX

Feed Task Type ○ Adhoc ● Recurring

Name * CbFeedDNS

URL * http://[redacted]/cbfeeddns.csv

□ Authenticated

□ Use proxy

Recur Every 4 Hour (s)

Date Range

Start Date 2018-01-25 11:50:21 End Date

Advanced Options

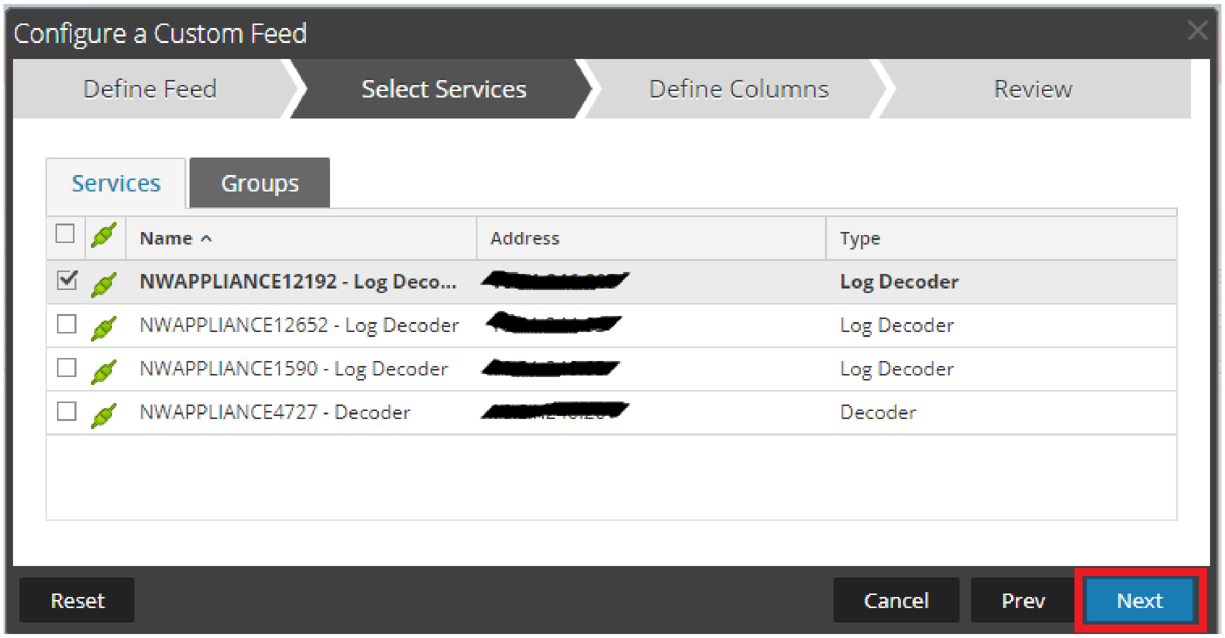
XML Feed File Select File

Separator ,

Comment #

f. Click **Next**.

g. To identify services on which to deploy the feed, select one or more Decoders, and click **Next**.

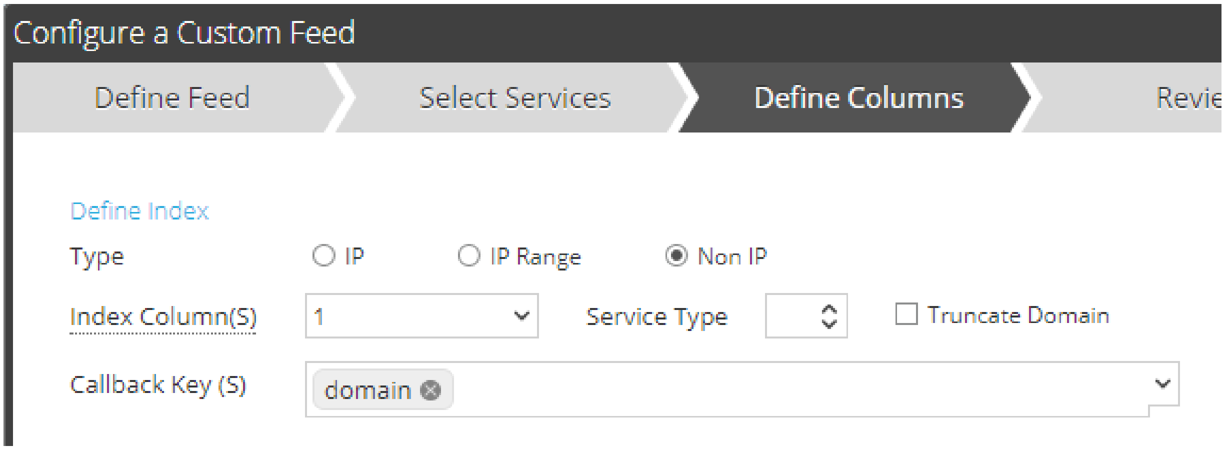


☐		Name ^	Address	Type
☑		NWAPPLIANCE12192 - Log Deco...	[redacted]	Log Decoder
☐		NWAPPLIANCE12652 - Log Decoder	[redacted]	Log Decoder
☐		NWAPPLIANCE1590 - Log Decoder	[redacted]	Log Decoder
☐		NWAPPLIANCE4727 - Decoder	[redacted]	Decoder

The Define Columns form is displayed.

h. In this example, we are using the DNS feed, which is non IP.

- Select **Non IP** for the Index type, and select **1** for the index column.
- Select **domain** for the Callback Key.

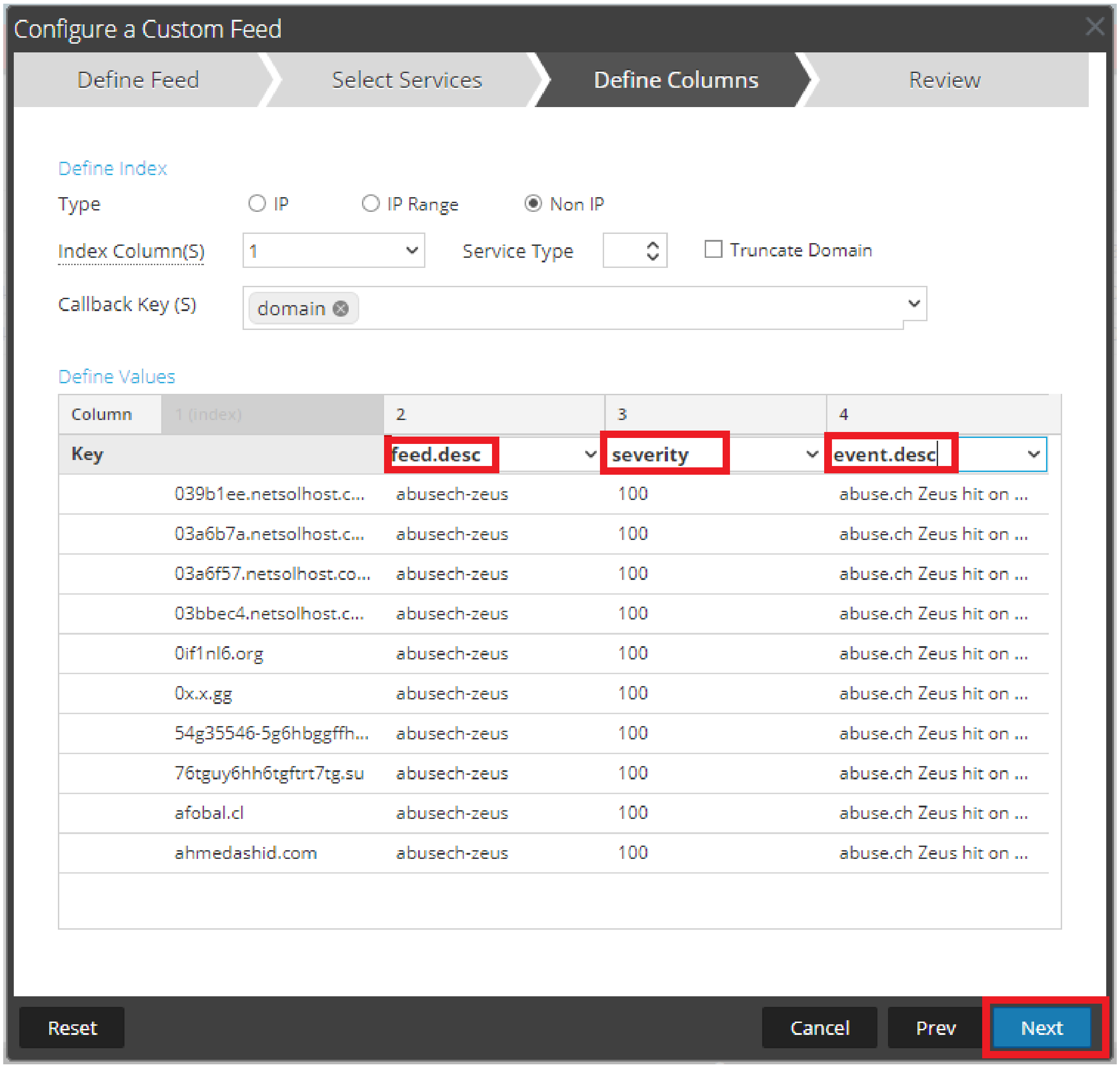


Type ○ IP ○ IP Range ● Non IP

Index Column(S) 1 Service Type ☐ Truncate Domain

Callback Key (S) domain

i. Add the keys and click **Next**.



Define Index

Type ○ IP ○ IP Range ● Non IP

Index Column(S): 1

Service Type

□ Truncate Domain

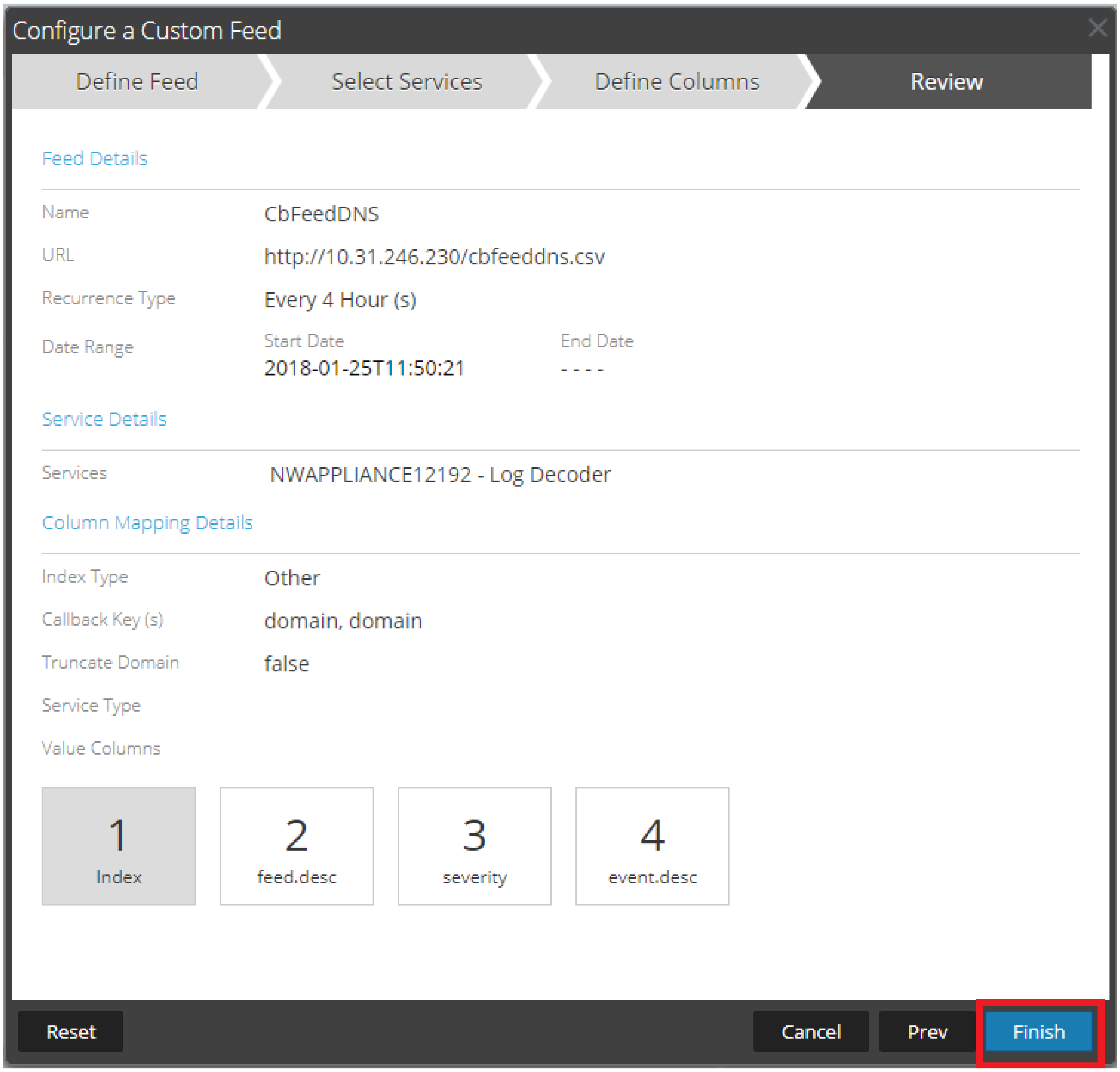
Callback Key (S): domain

Define Values

Column	1 (index)	2	3	4
Key		feed.desc	severity	event.desc
	039b1ee.netsolhost.c...	abusech-zeus	100	abuse.ch Zeus hit on ...
	03a6b7a.netsolhost.c...	abusech-zeus	100	abuse.ch Zeus hit on ...
	03a6f57.netsolhost.co...	abusech-zeus	100	abuse.ch Zeus hit on ...
	03bbec4.netsolhost.c...	abusech-zeus	100	abuse.ch Zeus hit on ...
	0if1nl6.org	abusech-zeus	100	abuse.ch Zeus hit on ...
	0x.x.gg	abusech-zeus	100	abuse.ch Zeus hit on ...
	54g35546-5g6hbggffh...	abusech-zeus	100	abuse.ch Zeus hit on ...
	76tguy6hh6tgftrt7tg.su	abusech-zeus	100	abuse.ch Zeus hit on ...
	afobal.cl	abusech-zeus	100	abuse.ch Zeus hit on ...
	ahmedashid.com	abusech-zeus	100	abuse.ch Zeus hit on ...

j. Click **Finish**.

The Review form is displayed. Your form should look like this:



Feed Details

Name	CbFeedDNS
URL	http://10.31.246.230/cbfeeddns.csv
Recurrence Type	Every 4 Hour (s)
Date Range	Start Date 2018-01-25T11:50:21
	End Date - - - -

Service Details

Services	NWAPPLIANCE12192 - Log Decoder

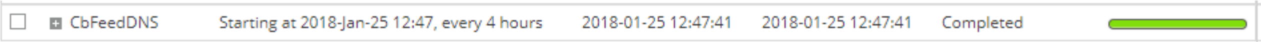
Column Mapping Details

Index Type	Other
Callback Key (s)	domain, domain
Truncate Domain	false
Service Type	
Value Columns	

1	2	3	4
Index	feed.desc	severity	event.desc

k. Review the feed information, and if correct, click **Finish**.

5. The page refreshes to show progress. When it is complete, you should see the following:



☐ ⊞ CbFeedDNS Starting at 2018-Jan-25 12:47, every 4 hours 2018-01-25 12:47:41 2018-01-25 12:47:41 Completed

Repeat this procedure for:

- **cbfeedipv4.csv**: use **IP** for feed type, and
- **cbfeedmd5.csv**: use **Non IP** for feed type.

Appendix A: Codes Samples and Other Reference Items

This Appendix contains code samples, configuration file listings, and other reference material that is part of the RSA NetWitness-Carbon Black Integration.

Cb Config Section

This is a listing of the Cb Config section of the `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` file.

```
# Raw Sensor (endpoint) Events
# Includes:
# ingress.event.process
# ingress.event.procstart
# ingress.event.netconn
# ingress.event.procend
# ingress.event.childproc
# ingress.event.moduleload
# ingress.event.module
# ingress.event.filemod
# ingress.event.regmod
# ingress.event.tamper
# ingress.event.crossprocopen
# ingress.event.remotethread
# ingress.event.processblock
# ingress.event.emetmitigation
# ALL for all of the above
# 0 - to disable all raw sensor events.
events_raw_sensor=ALL


# Watchlist Hits
# Includes:
# watchlist.hit.process
# watchlist.hit.binary
# watchlist.storage.hit.process
# watchlist.storage.hit.binary
# Note: As of version 5.2, the routing keys are different in RabbitMQ
# if you want to only subscribe to watchlist.storage.hit.process (for example),
# your configuration should be
# events_watchlist=watchlist.*.storage.hit.process note the '*' after the '.'
# Internally all watchlists show up with their database ID
# ex: watchlist.12.storage.hit.process, you'll miss them without the '*'
# (asterisk)
events_watchlist=ALL
```

```
# Feed Hits
# Includes:
# feed.ingress.hit.process
# feed.ingress.hit.binary
# feed.ingress.hit.host
# feed.storage.hit.process
# feed.storage.hit.binary
# feed.query.hit.process
# feed.query.hit.binary
# ALL for all of the above
# 0 - to disable all raw sensor events
# Note: As of version 5.2, the routing keys are different in RabbitMQ
# if you want to only subscribe to feed.storage.hit.process (for example), your
# configuration should be
# events_feed=feed.*.storage.hit.process note the '*' after the '.'
# Internally all feeds show up with their database ID
# ex: feed.12.storage.hit.process, you'll miss them without the '*' (asterisk)
events_feed=ALL


# Alert Events
# Includes:
# alert.watchlist.hit.ingress.process
# alert.watchlist.hit.ingress.binary
# alert.watchlist.hit.ingress.host
# alert.watchlist.hit.query.process
# alert.watchlist.hit.query.binary
# ALL for all of the above
# 0 - to disable all raw sensor events
events_alert=ALL


# Binary Observed Events
# Includes:
# binaryinfo.observed
# binaryinfo.host.observed
# binaryinfo.group.observed
events_binary_observed=ALL


# Binary Upload Events
# Includes:
# binarystore.file.added
events_binary_upload=ALL
```

Log Samples

This section contains logging information for sample events.

```
2017-09-13T10:57:47+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-
forwarder[10940]: LEEF:1.0|CB|CB|5.1|binarystore.file.added|cb_server=cbserver compressed_
size=1128 file_
```

```
path=/var/cb/data/modulestore/506/E6A/506E6A85E0CAED63C8D0B468C16D8C7A.zip
md5=506E6A85E0CAED63C8D0B468C16D8C7A node_id=0 size=2048
timestamp=1505280467.662 type=binarystore.file.added
```

```
2017-09-13T11:00:04+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-
forwarder[10940]: LEEF:1.0|CB|CB|5.1|watchlist.storage.hit.binary|cb_server=cbserver cb_version=612
company_name=Microsoft Corporation copied_mod_len=87040 digsig_publisher=Microsoft
Corporationdigsig_result=Signed digsig_result_code=0 digsig_sign_time=2012-08-17T01:50:00.000Z
endpoint=244APP198|1 event_partition_id=98640766238720 facet_id=808456 file_desc=Windows
Driver Foundation - User-mode Driver Framework Platform Driver file_version=6.2.9200.16384 (win8_
rtm.120725-1247) group=Default Group host_count=1 internal_name=WUDFPf.sys is_64bit=true is_
executable_image=true last_seen=2017-09-13T05:24:01.164Z legal_copyright=© Microsoft
Corporation. All rights reserved. md5=AB886378EEB55C6C75B4F2D14B6C869F observed_
filename=c:\\windows\\system32\\drivers\\wudfpf.sys orig_mod_len=87040 original_
filename=WUDFPf.sys os_type=Windows product_name=Microsoft® Windows® Operating System
product_version=6.2.9200.16384 server_added_timestamp=2017-09-13T05:23:49.883Z server_
name=localhost timestamp=1505280604.644 type=watchlist.storage.hit.binary watchlist_2=2017-09-
13T05:30:04.288954Z watchlist_id=2 watchlist_name=Newly Executed Applications
```

```
2017-09-13T11:00:05+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-
forwarder[10940]: LEEF:1.0|CB|CB|5.1|alert.watchlist.hit.query.binary|alert_severity=50.625 alert_
type=watchlist.hit.query.binary cb_server=cbserver computer_name=244APP198 created_time=2017-
09-13T05:30:05.144281Z digsig_result=Signed feed_id=-1 feed_name=My Watchlists feed_rating=3.0
host_count=1 hostname=244APP198 ioc_confidence=0.5 ioc_type=query
md5=6BCC1D7D2FD2453957C5479A32364E52 observed_filename=
["c:\\windows\\system32\\drivers\\ws2ifsl.sys"] observed_filename_total_count=1 os_type=Windows
other_hostnames=[] report_score=75 sensor_criticality=3.0 sensor_id=1 status=Unresolved
timestamp=1505280605.405 type=alert.watchlist.hit.query.binary unique_id=21ea29f2-5921-41d2-
be5d-5cc32c55a3c3 watchlist_id=2 watchlist_name=Newly Executed Applications
```

```
2017-09-21T13:50:05+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-
forwarder[10940]: LEEF:1.0|CB|CB|5.1|alert.watchlist.hit.query.binary|alert_severity=50.625 alert_
type=watchlist.hit.query.binary cb_server=cbserver computer_name=244APP198 created_time=2017-
09-21T08:20:05.687704Z digsig_result=Signed feed_id=-1 feed_name=My Watchlists feed_rating=3.0
host_count=1 hostname=244APP198 ioc_confidence=0.5 ioc_type=query
md5=F96CF9925A0C5948AB9B100E43148FC7 observed_filename=
["c:\\windows\\system32\\jscript9.dll"] observed_filename_total_count=1 os_type=Windows other_
hostnames=[] report_score=75 sensor_criticality=3.0 sensor_id=1 status=Unresolved
timestamp=1505982005.78 type=alert.watchlist.hit.query.binary unique_id=e06b678b-b824-428d-
9559-5a7a73aa8b68 watchlist_id=6 watchlist_name=Newly Loaded Modules
```

```
2017-10-23T14:20:06+05:30 cbintegration /usr/share/cb/integrations/event-forwarder/cb-event-
```

```
forwarder[15552]: LEEF:1.0|CB|CB|5.1|alert.watchlist.hit.query.process|alert_severity=50.625 alert_
type=watchlist.hit.query.process cb_server=cbserver childproc_count=2 comms_ip=10.31.244.198
computer_name=244app198 created_time=2017-10-23T08:50:06.344786Z crossproc_count=2 feed_
id=-1 feed_name=My Watchlists feed_rating=3.0 filemod_count=9 group=default group
hostname=244app198 interface_ip=10.31.244.198 ioc_attr={"highlights":
["c:\\\\windows\\\\system32\\\\PREPREPREnotepad.exePOSTPOSTPOST"]} ioc_confidence=0.5 ioc_
type=query md5=852D67A27E454BD389FA7F02A8CBE23F modload_count=73 netconn_count=0
os_type=windows process_guid=00000001-0000-0888-01d3-4bd996561462 process_id=00000001-
0000-0888-01d3-4bd996561462 process_name=powershell.exe process_
path=c:\\windows\\system32\\windowspowershell\\v1.0\\powershell.exe process_unique_
id=00000001-0000-0888-01d3-4bd996561462-015f4863c908 regmod_count=1 report_score=75
segment_id=1 sensor_criticality=3.0 sensor_id=1 status=Unresolved timestamp=1508748606.459
type=alert.watchlist.hit.query.process unique_id=655fab45-ab91-48b9-99c3-e30a0392959c
username=ABHIDC\\Administrator watchlist_id=9 watchlist_name=Test
```

List of Files Delivered in the ZIP Archive

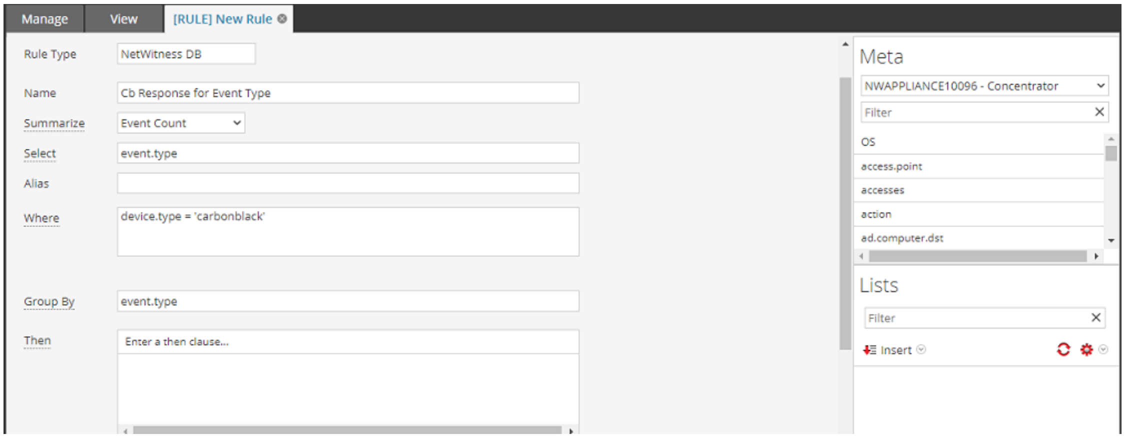
The **Cb Response Interop.zip** archive contains the following:

- Charts
  - Cb Response for Action
  - Cb Response for Alert Type
  - Cb Response for Event Type
  - Cb Response for Filename
  - Cb Response for Process
  - Cb Response for Severity
- Rules
  - Cb Response Filename
  - Cb Response for Action
  - Cb Response for Alert Type
  - Cb Response for Event Type
  - Cb Response for Process
  - Cb Response for Severity

The **Cb+Response+Interop.cfg** contains the information you need to import the Cb Response Interop Dashboard.

Samples screens:

- Sample screen for building one of the rules:



Rule Type: NetWitness DB

Name: Cb Response for Event Type

Summarize: Event Count

Select: event.type

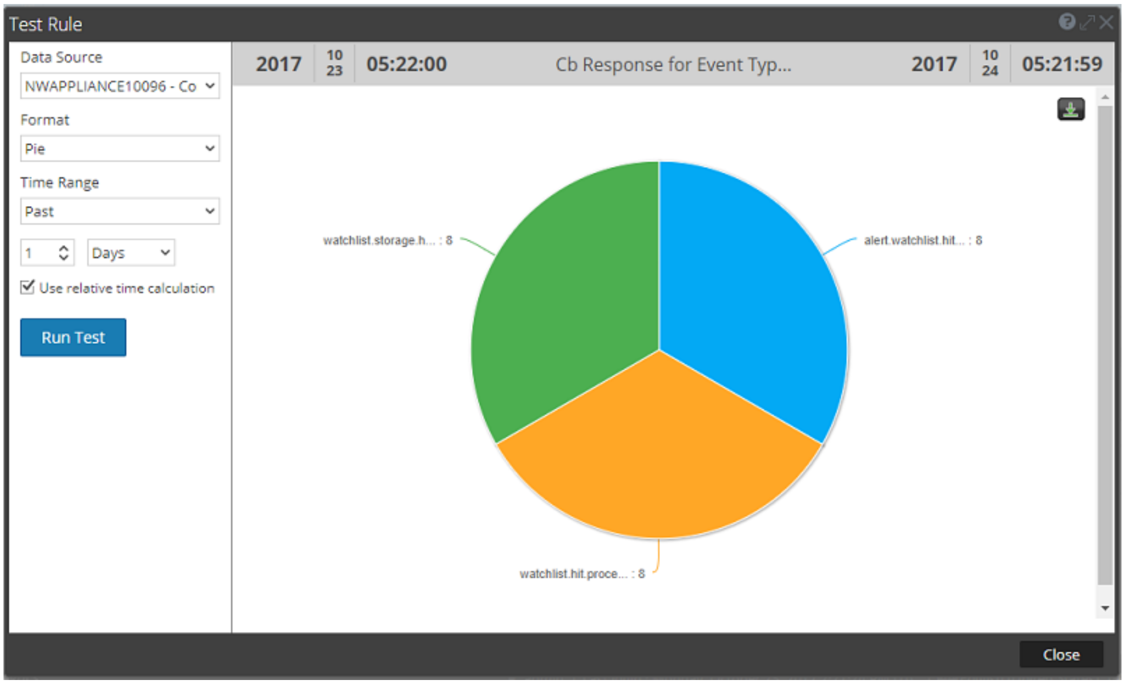
Alias:

Where: device.type = 'carbonblack'

Group By: event.type

Then: Enter a then clause...

- Sample screen for testing one of the rules:



Test Rule

Data Source: NWAPPLIANCE10096 - Co

Format: Pie

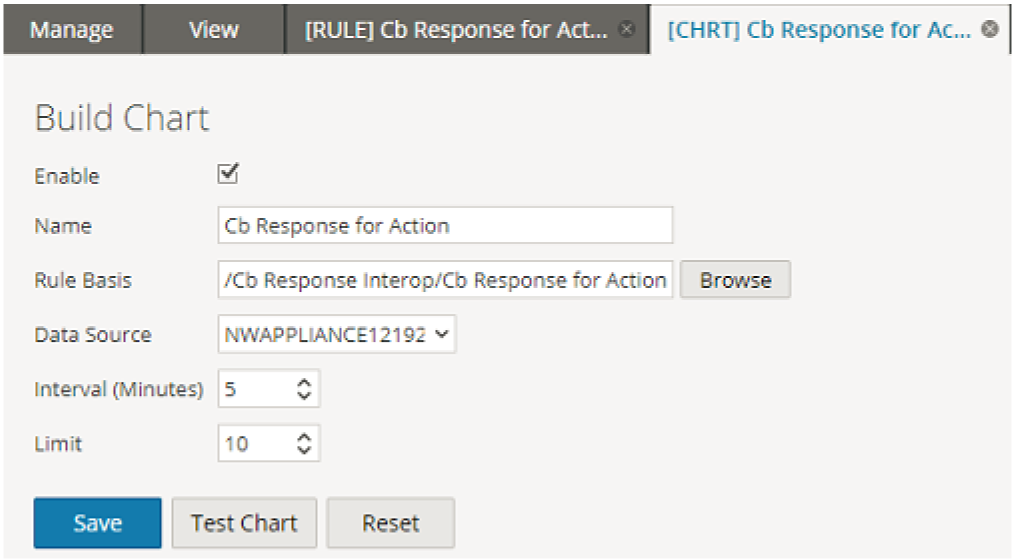
Time Range: Past

1 Days

☑ Use relative time calculation

Run Test
2017
10
23
05:22:00
Cb Response for Event Typ...
2017
10
24
05:21:59
watchlist.storage.h... : 8
alert.watchlist.hit... : 8
watchlist.hit.proce... : 8
Close

- Sample screen for building one of the charts:



Build Chart

Enable ☑

Name: Cb Response for Action

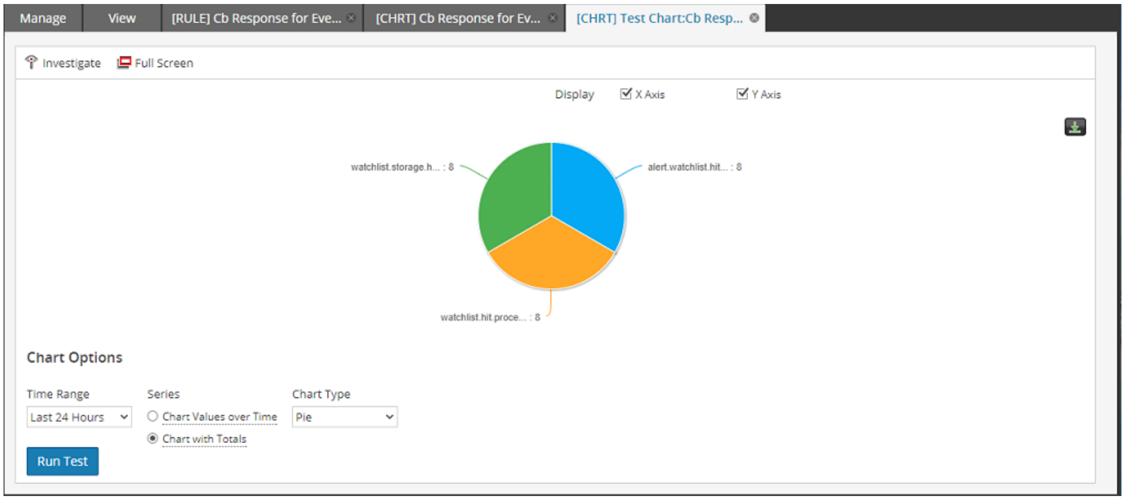
Rule Basis: /Cb Response Interop/Cb Response for Action

Data Source: NWAPPLIANCE12192

Interval (Minutes): 5

Limit: 10

- Sample screen for testing a chart:


Manage
View
[RULE] Cb Response for Eve...
[CHRT] Cb Response for Ev...
[CHRT] Test Chart:Cb Resp...
Investigate
Full Screen
watchlist.storage.h... : 8
alert.watchlist.hit... : 8
watchlist.hit.proce... : 8
Run Test

Display ☑ X Axis ☑ Y Axis

Chart Options

Time Range: Last 24 Hours

Series: ○ Chart Values over Time ● Chart with Totals

Chart Type: Pie

Appendix B: Manually Create Rules, Charts and Dashboard

These are the steps to manually create the dashboard, and the rules and charts it uses:

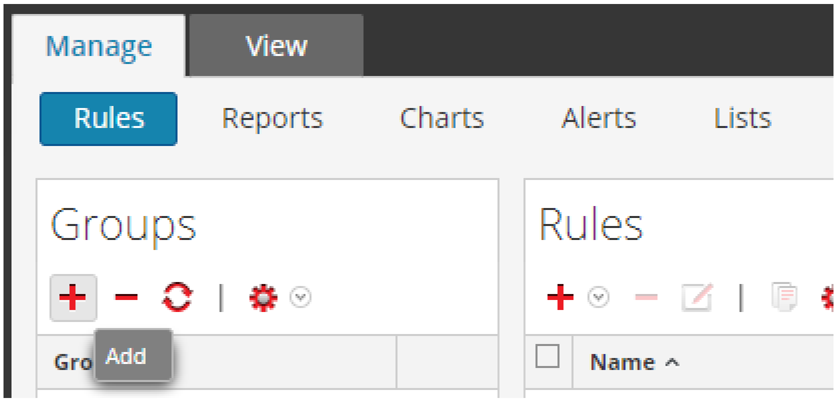
1. Create the Rules Group
2. Build and test Rules and Charts. Repeat these steps for each of the 6 rules and charts.
3. Create the Charts Group
4. Create Dashboard with Dashlets

Note: Remember, you can import the **Cb Response Interop.zip** archive to automatically import the rules and charts. And you can use the **Cb+Response+Interop.cfg** file to automatically add the corresponding dashboard.

Create Rules Group

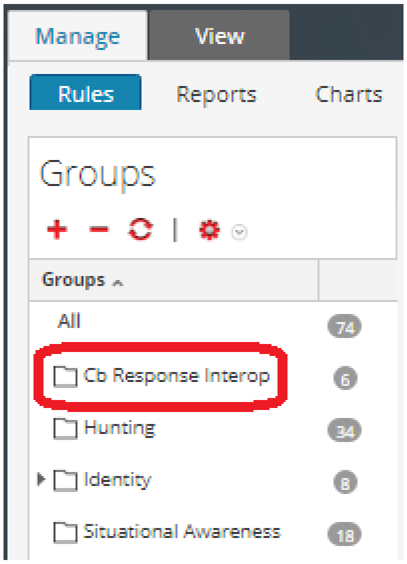
To create the rules group:

1. From RSA NetWitness UI, go to **MONITOR** > **Reports**.
2. In the **Manage** tab, click **Rules**.
3. In the Groups pane, click +.



4. Enter **Cb Response Interop** for the new group name.

The new group is listed in the Groups pane:



Proceed to the next section to add rules and charts.

Build and test a Rule and Chart

This procedure uses the **Cb Response for Event Type** as an example. You will repeat this procedure for each of the other Cb Response rules.

To create the Cb Response for Event Type rule and chart:

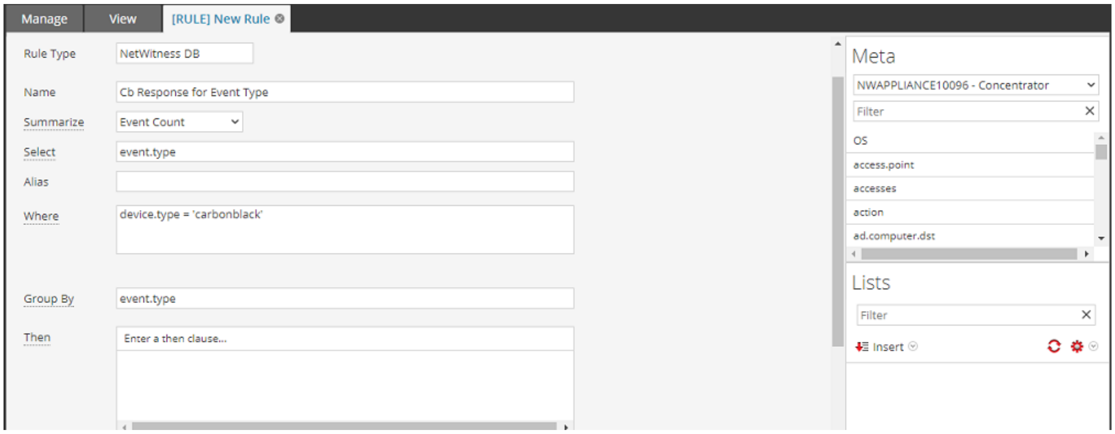
1. Go to **MONITOR > Reports**, then in the **Manage** tab, make sure the **Rules** tab is selected.
2. In the Groups pane, select the **Cb Response Interop** group.
3. In the Rules tab, click + ⌄ > **NetWitness Suite DB** from the Rules toolbar.

   A new Build Rule tab is displayed.
4. From the Build new Rule tab, fill in the following information:

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**
Name	Enter **Cb Response for Event Type**
Summarize	Select **Event Count**

Field	Value
Select	Enter **event.type**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

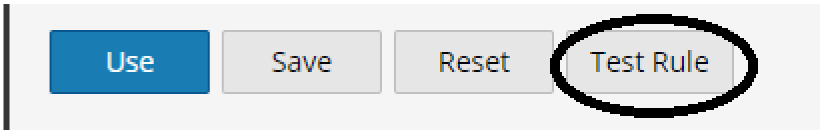
5. In the Meta pane, in the top field, select a concentrator.



Rule Type: NetWitness DB
Name: Cb Response for Event Type
Summarize: Event Count
Select: event.type
Alias:
Where: device.type = 'carbonblack'
Group By: event.type
Then: Enter a then clause...
Meta: NWAPPLIANCE10096 - Concentrator

6. Click **Save**.

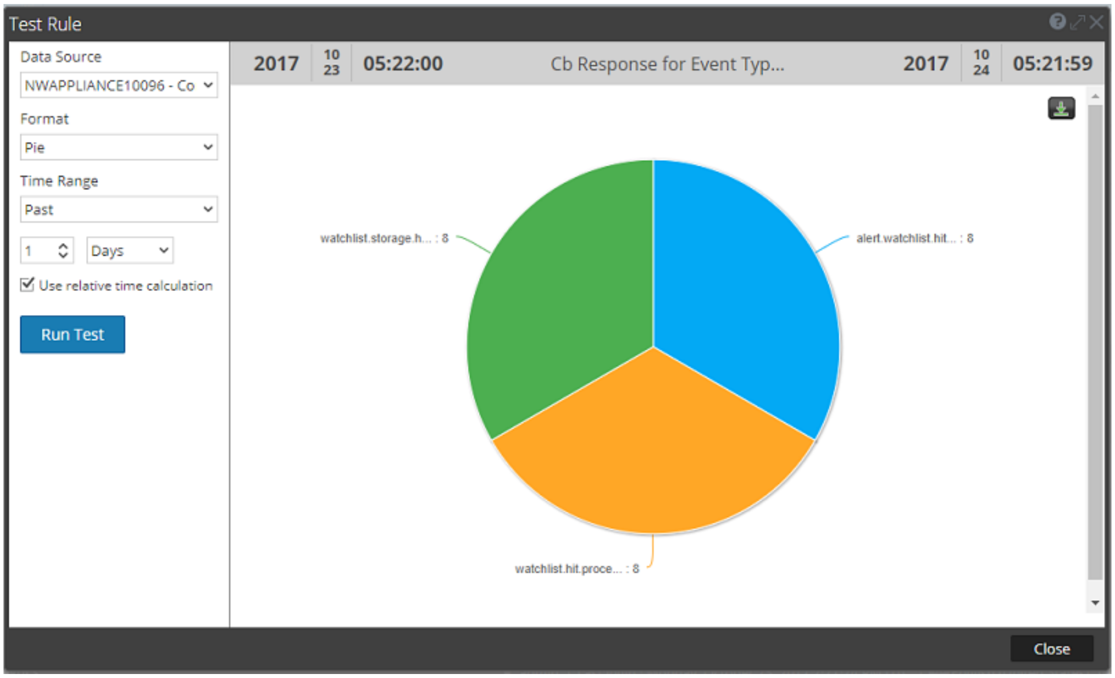
7. Click Test Rule.



8. In the Test Rule dialog box, select the **Format**, **Time Range** the **Use relative time calculation** box.

9. Click Run Test.

   This is an example test run:


Test Rule
Run Test
2017 10 23 05:22:00
Cb Response for Event Typ...
2017 10 24 05:21:59
watchlist.storage.h... : 8
alert.watchlist.hit... : 8
watchlist.hit.proce... : 8
Close

Data Source
NWAPPLIANCE10096 - Co

Format
Pie

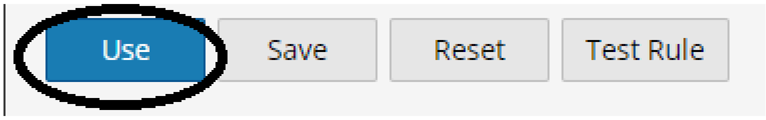
Time Range
Past

1 Days

☑ Use relative time calculation

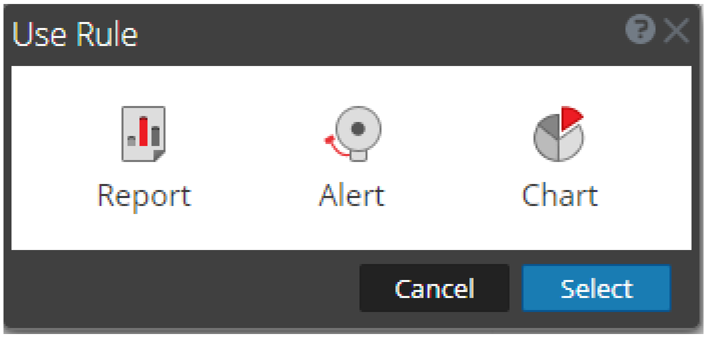
10. Click **Close** to close the Test Rule dialog box.

11. Click **Use**.



The Use Rule dialog box is displayed.

12. In the Use Rule dialog box, click **Chart**.



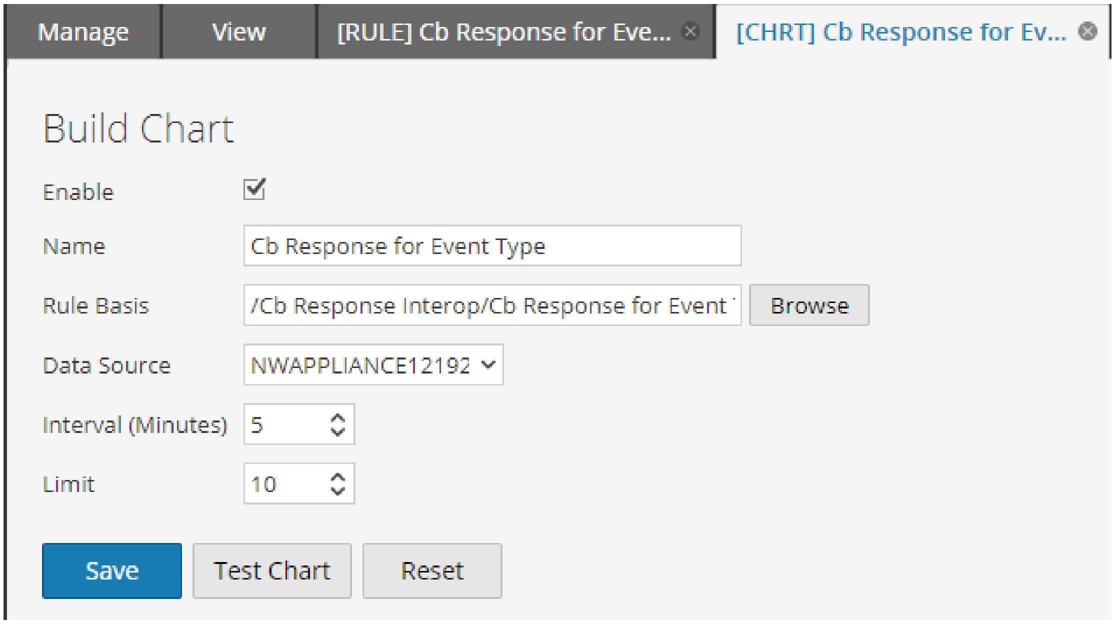
13. Click **Select**.

A new Build Chart dialog box is displayed.

14. From the Build new Chart tab, fill in the following information:

Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Event Type**
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)
Limit	Accept the default value (10)

The screen should look similar to the following:



Build Chart

Enable ☑

Name: Cb Response for Event Type

Rule Basis: /Cb Response Interop/Cb Response for Event

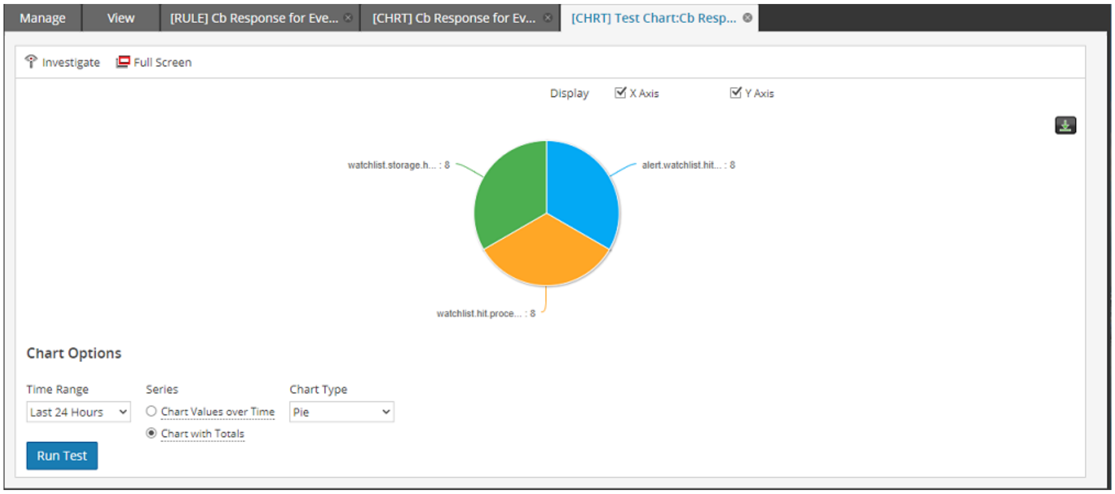
Data Source: NWAPPLIANCE12192

Interval (Minutes): 5

Limit: 10

15. Click **Save**.
16. Click **Test Chart**.
17. In the Test Chart dialog box, select the following:
    - Select a date range
    - Select the **Series**
    - Select a **Chart Type**
18. Click Run Test.

    This is an example test run:


Manage
View
[RULE] Cb Response for Eve...
[CHRT] Cb Response for Ev...
[CHRT] Test Chart:Cb Resp...
Investigate
Full Screen
watchlist.storage.h... : 8
alert.watchlist.hit... : 8
watchlist.hit.proce... : 8
Run Test

Display ☑ X Axis ☑ Y Axis

Chart Options

Time Range: Last 24 Hours

Series: ○ Chart Values over Time ● Chart with Totals

Chart Type: Pie

19. Click **Close** to close the Test Chart tab.

Build and test the Other Rules and Charts

In the previous section, previous section, Build and test a Rule and Chart, we walked through the steps to build the **Cb Response for Event Type** chart and rule. The procedure to create the remaining rules and charts is the same as shown in that section. The only differences are in step 4, where you enter the details for the rule, and step 14, where you enter the details for the corresponding chart.

Repeat the previous procedure for each of the remaining rules and charts:

- Cb Response for Action
- Cb Response for Alert Type
- Cb Response for Filename
- Cb Response for Process
- Cb Response for Severity

Cb Response for Action

In the Build Rule tab, enter the following information.

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**

Field	Value
Name	Enter **Cb Response for Action**
Summarize	Select **Event Count**
Select	Enter **action**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

In the Build Chart tab, enter the following information.

Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Action**
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)
Limit	Accept the default value (10)

Cb Response for Alert Type

In the Build Rule tab, enter the following information.

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**
Name	Enter **Cb Response for Alert Type**
Summarize	Select **Event Count**
Select	Enter **alert**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

In the Build Chart tab, enter the following information.

Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Alert Type**
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)
Limit	Accept the default value (10)

Cb Response for Filename

In the Build Rule tab, enter the following information.

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**
Name	Enter **Cb Response for Filename**
Summarize	Select **Event Count**
Select	Enter **filename**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

In the Build Chart tab, enter the following information.

Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Filename**
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)

Field	Value
Limit	Accept the default value (10)

Cb Response for Process

In the Build Rule tab, enter the following information.

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**
Name	Enter **Cb Response for Process**
Summarize	Select **Event Count**
Select	Enter **process**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

In the Build Chart tab, enter the following information.

Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Filename**

Field	Value
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)
Limit	Accept the default value (10)

Cb Response for Severity

In the Build Rule tab, enter the following information.

Field	Value
Rule Type	You cannot edit this field. • For NW 11.x this value is **NetWitness Suite DB** • For SA 10.x this value is **NetWitness Db**
Name	Enter **Cb Response for Severity**
Summarize	Select **Event Count**
Select	Enter **severity**
Alias	leave blank
Where	Enter **device.type = 'carbonblack'**
Group By	You cannot edit this field: it is automatically filled from the value you entered in the **Select** field.
Order By	Select **Total** for the Column Name and **Ascending** for Sort By
Session Threshold	Enter **500**
Limit	Enter **5000**

In the Build Chart tab, enter the following information.

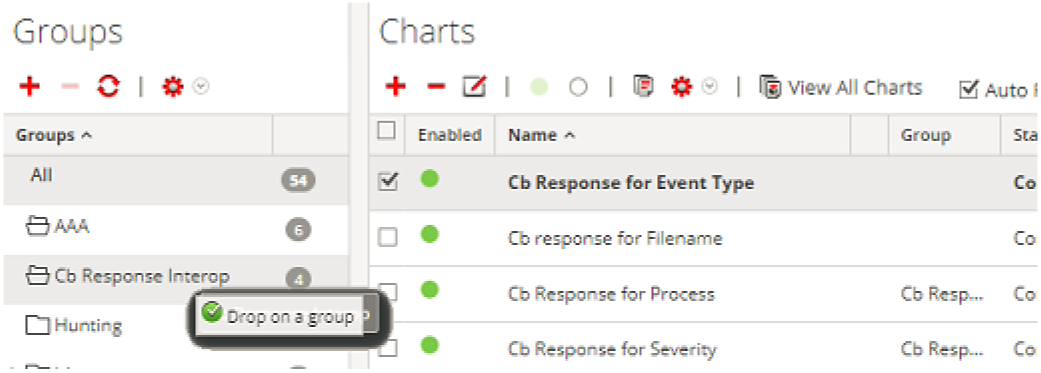
Field	Value
Enable	Make sure this is selected.
Name	Enter **Cb Response for Severity**
Rule Basis	This field is auto filled with the name of the corresponding rule.
Data Source	Should already be filled; if not, select a Concentrator service.
Interval	Accept the default value (5 minutes)
Limit	Accept the default value (10)

Create Charts Group

To create the charts group:

1. From RSA NetWitness UI, go to **MONITOR > Reports**.
2. In the **Manage** tab, click **Charts**.
3. In the Groups pane, click + .
4. Enter **Cb Response Interop** for the new group name.

   The new group is listed in the Groups pane.
5. Select **All** in the Groups pane.
6. Select one of the Cb Response charts, and drag-and-drop into the **Cb Response Interop** charts group:

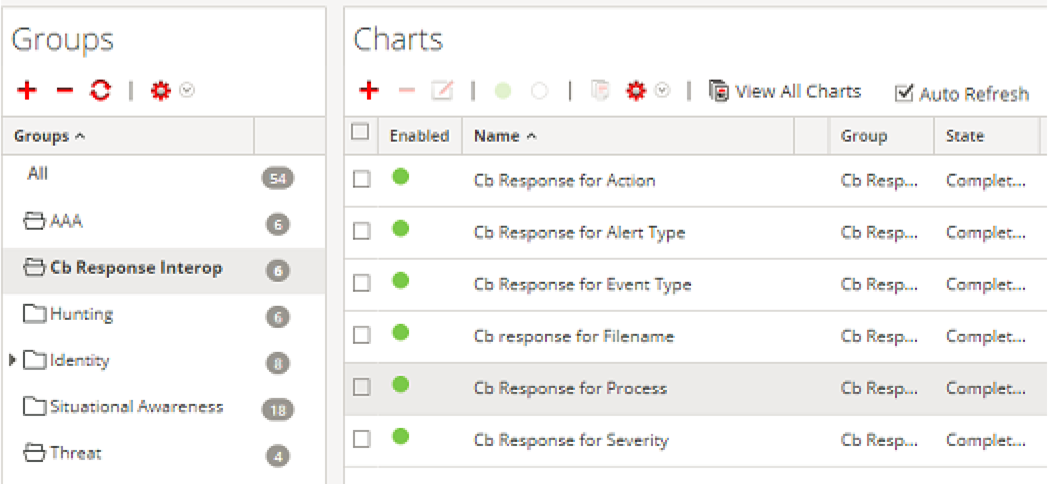


Groups	
All	54
AAA	6
Cb Response Interop	4
Hunting	

☐	Enabled	Name	Group	Sta
☑	●	Cb Response for Event Type		Co
☐	●	Cb response for Filename		Co
☐	●	Cb Response for Process	Cb Resp...	Co
☐	●	Cb Response for Severity	Cb Resp...	Co

7. Repeat step 6 for all of the Cb Response Interop charts, until the screen looks similar to the

following:



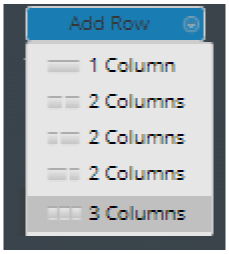
Groups ^	
All	54
AAA	6
Cb Response Interop	6
Hunting	6
Identity	8
Situational Awareness	18
Threat	4

□	Enabled	Name ^	Group	State
□	●	Cb Response for Action	Cb Resp...	Complet...
□	●	Cb Response for Alert Type	Cb Resp...	Complet...
□	●	Cb Response for Event Type	Cb Resp...	Complet...
□	●	Cb response for Filename	Cb Resp...	Complet...
□	●	Cb Response for Process	Cb Resp...	Complet...
□	●	Cb Response for Severity	Cb Resp...	Complet...

Create Dashboard with Dashlets

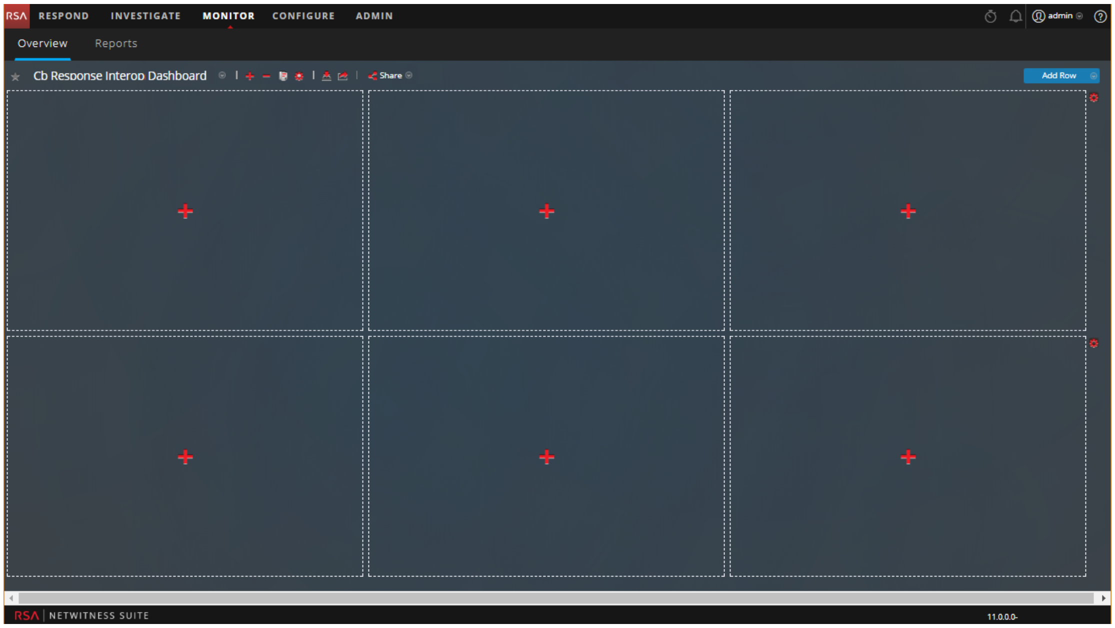
To create the dashboard and dashlets:

1. From RSA NetWitness UI, go to **MONITOR** > **Overview**.
2. In the Dashboard toolbar, click +.
3. In the Create a Dashboard dialog box, enter **Cb Response Interop**.
4. In the Add Row dialog box, select 3 columns.



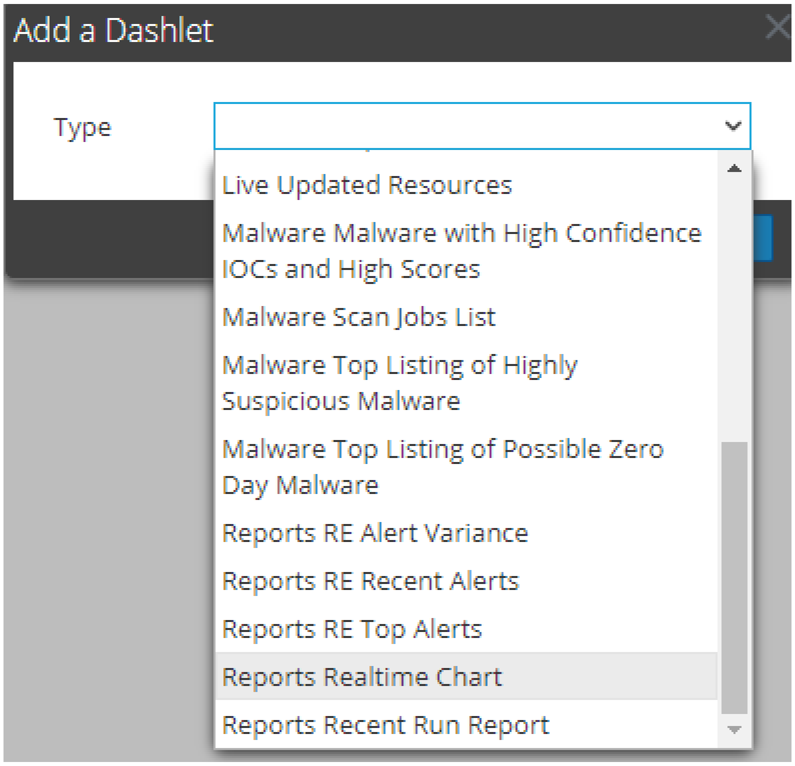
5. Repeat this step, adding another 3-column row.

   Your screen should now have 6 empty cells for the dashlets:



6. Perform the following steps to add the first dashlet:

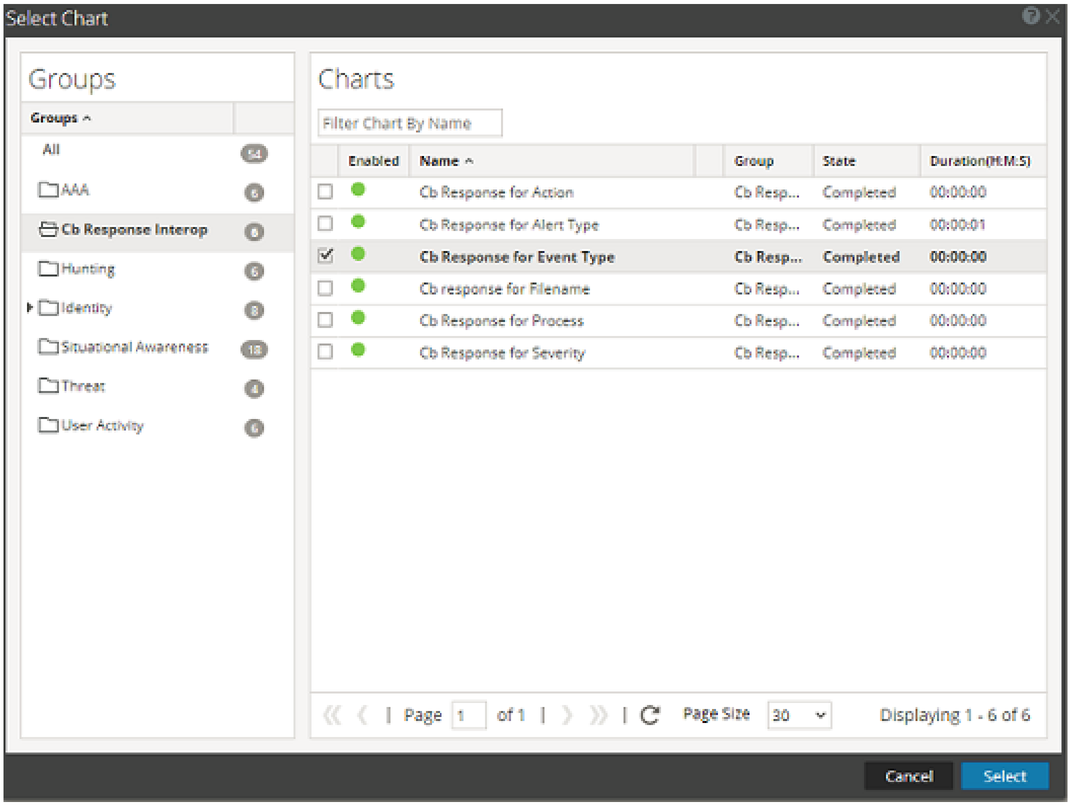
   a. Click inside the top left cell, and in the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.


Add a Dashlet
Type
Live Updated Resources
Malware Malware with High Confidence IOCs and High Scores
Malware Scan Jobs List
Malware Top Listing of Highly Suspicious Malware
Malware Top Listing of Possible Zero Day Malware
Reports RE Alert Variance
Reports RE Recent Alerts
Reports RE Top Alerts
Reports Realtime Chart
Reports Recent Run Report

   b. For the **Chart** field, click the **Browse** button to open the Select Chart dialog box.

   c. Select the Cb Response Interop group in the Groups pane, and choose the **Cb Response**

for Event Type chart.



Select Chart

Groups

Groups ^	
All	54
AAA	6
Cb Response Interop	6
Hunting	6
Identity	8
Situational Awareness	18
Threat	4
User Activity	6

Charts

Filter Chart By Name

	Enabled	Name ^	Group	State	Duration(H:M:S)
□	●	Cb Response for Action	Cb Resp...	Completed	00:00:00
□	●	Cb Response for Alert Type	Cb Resp...	Completed	00:00:01
☑	●	**Cb Response for Event Type**	**Cb Resp...**	**Completed**	**00:00:00**
□	●	Cb response for Filename	Cb Resp...	Completed	00:00:00
□	●	Cb Response for Process	Cb Resp...	Completed	00:00:00
□	●	Cb Response for Severity	Cb Resp...	Completed	00:00:00

Page 1 of 1 Page Size 30 Displaying 1 - 6 of 6

d. Click Select.

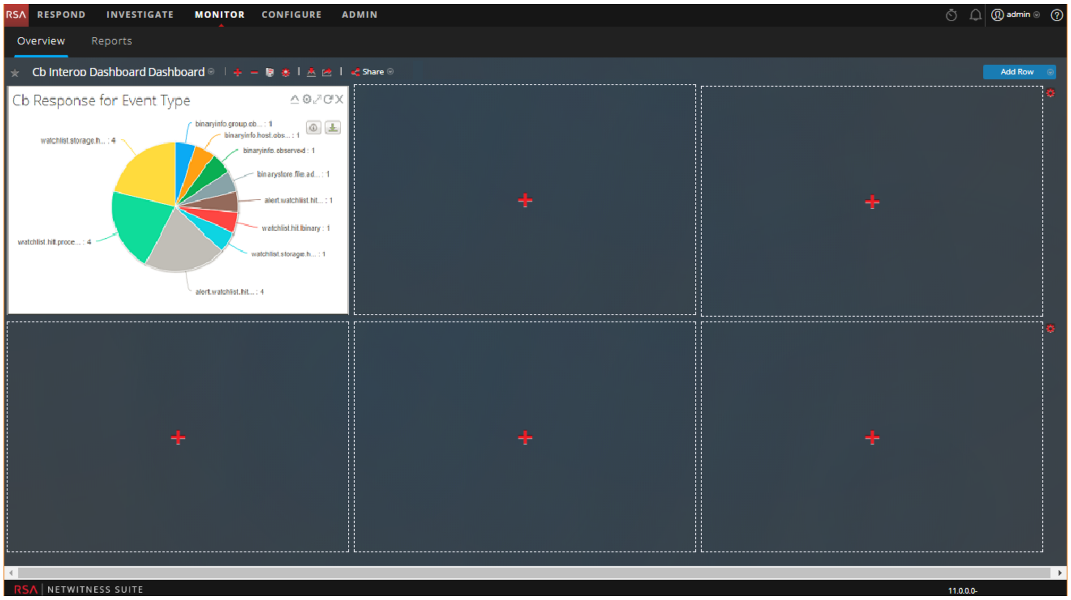
You are returned to the **Add a Dashlet** dialog box.

e. Fill in the following values:

- For **Series**, choose **Chart with Totals**.
- For **Chart Type**, select **Pie**.
- Select **Past Hours** and **Refresh Interval** as deemed fit.

f. Click **Add**.

The dashlet is added to the dashboard.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Overview
Reports
Cb Interop Dashboard Dashboard
Share
Add Row
Cb Response for Event Type
binaryinfo.group.ob... : 1
binaryinfo.host.obs... : 1
binaryinfo.observed : 1
binarystore.file.ad... : 1
alert.watchlist.hit... : 1
watchlist.hit.binary : 1
watchlist.storage.h... : 1
alert.watchlist.hit... : 4
watchlist.hit.proce... : 4
watchlist.storage.h... : 4
RSA | NETWITNESS SUITE
11.0.0.0-

Repeat steps 6.a – 6.f to create the 5 remaining dashlets, add the values as described below.

Add the filename dashlet:

- In the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.
- Select the Select the **Cb Response for Filename** chart.
- Fill in the following values in the **Add a Dashlet** dialog box:
  - For **Series**, choose **Chart with Totals**.
  - For **Chart Type**, select **Column**.
  - Select **Past Hours** and **Refresh Interval** as deemed fit.

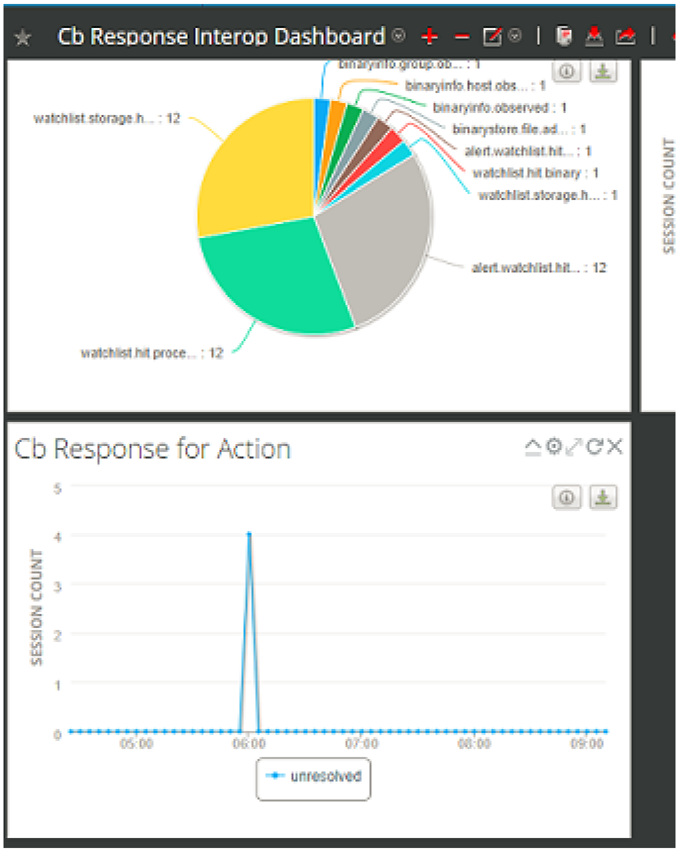
Add the process dashlet:

- In the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.
- Select the Select the **Cb Response for Process** chart.
- Fill in the following values in the **Add a Dashlet** dialog box:
  - For **Series**, choose **Chart with Totals**.
  - For **Chart Type**, select **Column**.
  - Select **Past Hours** and **Refresh Interval** as deemed fit.

Add the action dashlet:

- In the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.
- Select the Select the **Cb Response for Action** chart.
- Fill in the following values in the **Add a Dashlet** dialog box:
  - For **Series**, choose **Chart Values over Time**.
  - For **Top**, enter 10.
  - For **Chart Type**, select **Line**.
  - Select **Past Hours** and **Refresh Interval** as deemed fit.

  At this point, the left portion of the dashboard should look similar to the following:


Cb Response Interop Dashboard
binaryinfo.group.ob... : 1
binaryinfo.host.obs... : 1
binaryinfo.observed : 1
binarystore.file.ad... : 1
alert.watchlist.hit... : 1
watchlist.hit.binary : 1
watchlist.storage.h... : 1
watchlist.storage.h... : 12
alert.watchlist.hit... : 12
watchlist.hit.proce... : 12
SESSION COUNT
Cb Response for Action
5
4
3
2
1
0
SESSION COUNT
05:00
06:00
07:00
08:00
09:00
unresolved

Add the alert dashlet:

- In the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.
- Select the Select the **Cb Response for Alert Type** chart.
- Fill in the following values in the **Add a Dashlet** dialog box:

  - For **Series**, choose **Chart with Totals**.
  - For **Chart Type**, select **Pie**.
  - Select **Past Hours** and **Refresh Interval** as deemed fit.

Add the severity dashlet:

- In the **Add a Dashlet** dialog box, select **Reports Realtime Charts**.
- Select the Select the **Cb Response for Severity** chart.
- Fill in the following values in the **Add a Dashlet** dialog box:
  - For **Series**, choose **Chart Values over Time**.
  - For **Top**, enter 10.
  - For **Chart Type**, select **Line**.
  - Select **Past Hours** and **Refresh Interval** as deemed fit.