RSA NETWITNESS® PLATFORM

Automated Threat Detection Configuration Guide

for RSA NetWitness® Platform 11.3

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

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

April 2019

Contents

NetWitness Platform Automated Threat Detection

RSA NetWitness® Platform Automated Threat Detection uses preconfigured ESA Analytics modules to identify specific types of threats. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics modules reside within ESA Analytics services. The ESA Analytics services use query-based aggregation (QBA) to collect filtered events for the modules from Concentrators. Only the data required by a module is transferred between the Concentrator and the ESA Analytics system.

There are two ESA services that can run on an ESA host:

- ESA Correlation (ESA Correlation rules)
- Event Stream Analytics Server (ESA Analytics)

The first service is the ESA Correlation service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live. The second service is the ESA Analytics service, which is used for Automated Threat Detection. Because the ESA Analytics service uses preconfigured modules for Automated Threat Detection, you do not have to create or download rules to use Automated Threat Detection.

> **Note:** The Contexthub Server service, which provides enrichment lookup capability in the Respond and Investigate views, runs only on an ESA Primary host. For information, see the *Context Hub Configuration Guide*.

NetWitness Platform Automated Threat Detection currently has two Suspicious Domain modules available, Command and Control (C2) for Packets and C2 for Logs.

Because each ESA Analytics module has different data requirements, be sure that all module-specific requirements are met before you deploy a module for Automated Threat Detection.

Automated Threat Detection for Suspicious Domains

The Suspicious Domains modules examine your HTTP traffic to detect domains likely to be malware Command and Control servers connecting to your environment. After NetWitness Platform Automated Threat Detection for Suspicious Domains examines your HTTP traffic, it generates scores based on various aspects of your traffic behavior (such as the frequency and regularity with which a given domain is contacted). If these scores reach a set threshold, an ESA alert is generated. This ESA alert is forwarded to the Respond view. The alert in the Respond view is enriched with data that helps you to interpret the scores to determine what mitigation steps to take.

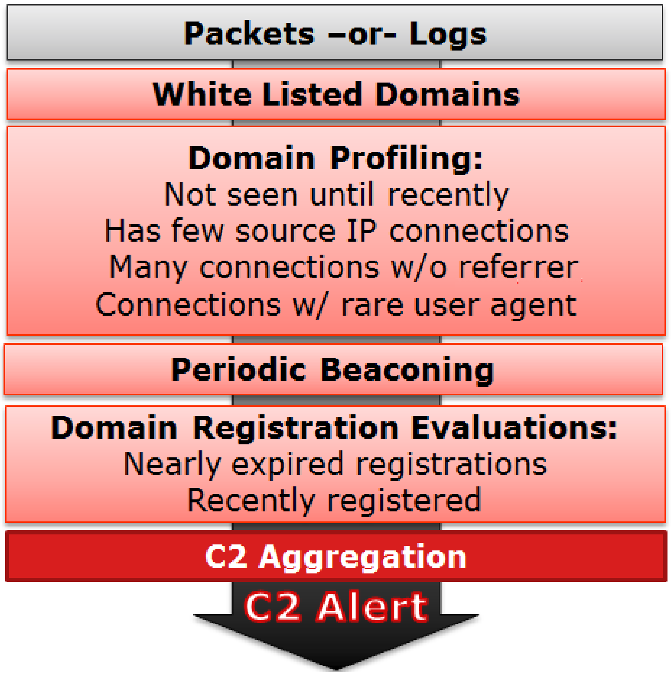
The Automated Threat Detection Suspicious Domain modules provide scoring to detect Command and Control communications. Command and Control communications occur when malware has compromised a system and is sending data back to a source. Often, Command and Control malware can be detected via beaconing behavior. Beaconing occurs when the malware regularly sends communications back to the Command and Control server to notify it that a machine has been compromised and the malware is awaiting further instructions. The ability to catch the malware at this stage of compromise can prevent any further harm from occurring to the compromised machine and is considered a critical stage in the "kill chain."

NetWitness Platform Automated Threat Detection solves several common problems that occur when searching for malware:

- **Ability to use algorithms rather than signatures**. Because many malware creators have begun using polymorphic or encrypted code segments, which are very difficult to create a signature for, this approach can sometimes miss malware. Because NetWitness Platform Automated Threat Detection uses a behavior-based algorithm, it is able to detect malware more quickly and effectively.
- **Ability to automate hunting**. Hunting through data manually is an effective but extremely time-consuming method of finding malware. Automating this process allows an analyst to use his or her time more effectively.
- **Ability to find an attack quickly**. Instead of batching and then analyzing the data, Automated Threat Detection analyzes data as it is ingested by NetWitness Platform, allowing for the attacks to be found in near real time.

Suspicious Domains Module Workflow

NetWitness Platform Automated Threat Detection works much like a filtering system. It checks to see if certain behavior occurs (or certain conditions exist), and if that behavior or condition occurs, it moves to the next step in the process. This helps to make the system efficient, and frees up resources so that events that are determined to be non-threatening are not held in memory. The following diagram provides a simplified version of the Suspicious Domains module workflow.


Packets –or- Logs
White Listed Domains
Domain Profiling:
Not seen until recently
Has few source IP connections
Many connections w/o referrer
Connections w/ rare user agent
Periodic Beaconing
Domain Registration Evaluations:
Nearly expired registrations
Recently registered
C2 Aggregation
C2 Alert

1.) **Packets or logs are routed to the ESA**. The HTTP packets or logs are parsed by the Decoder or Log Decoder and sent to the ESA host.

2.) **Whitelist is checked**. If you created a whitelist through the Context Hub, ESA checks this list to rule out domains. If a domain in the event is whitelisted, the event is ignored.

3.) **The domain profile is checked**. Automated Threat Detection checks to see if the domain is newly seen (approximately three days), has few source IP connections, has many connections without a referer, or has connections with a rare user agent. If one or several of these conditions is true, the domain is next checked for periodic beaconing.

4.) **The domain is checked for periodic beaconing**. Beaconing occurs when the malware regularly sends communications back to the command and control server to notify it that a machine has been compromised and the malware is awaiting further instructions. If the site displays beaconing behavior, then the domain registration information is checked.

5.) **Domain registration information is checked**. The Whois service is used to see if the domain is recently registered or nearly expired. Domains that have a very short lifespan are often hallmarks of malware.

6.) **Command and Control (C2) aggregates scores**. Each of the above factors generates a separate score, which is weighted to indicate various levels of importance. The weighted scores determine if an alert should be generated. If an alert is generated, the aggregated alerts appear in the Respond view and can then be investigated further from there. Once the alerts begin to appear in the Respond view, they continue to aggregate under the associated incident. This makes it easier to sort through volumes of alerts that can be generated for a command and control incident.

Analysts can view the alerts in the Respond view.

Suspicious Domains Automated Threat Detection on Packets vs. Web Proxy Logs

RSA NetWitness Platform provides you with the ability to perform Automated Threat Detection for Suspicious Domains using either packets or web proxy logs. While packet data can be streamed directly off of the wire into the NetWitness Platform installation and analyzed directly, if you have the ability to use a web proxy in your installation it may be beneficial to use it. Because some installations use network translation or SSL encryption, the true source IP of an outgoing connection may be masked if you are observing it at the packet level. By using a web proxy you gain the benefit of its ability to accelerate and decrypt SSL traffic as well as its ability to track the true source IP addresses of traffic it monitors.

Both Suspicious Domains for Packets (C2 for Packets) and Suspicious Domains for Logs (C2 for Logs) should produce the same results. From a results point of view, there is no real advantage to using one over the other.

Configuring Automated Threat Detection for Suspicious Domains

This topic tells administrators and analysts how to configure a Suspicious Domains module for NetWitness Platform Automated Threat Detection. The Automated Threat Detection functionality enables you to analyze the data that resides on one or more Concentrators by using preconfigured ESA Analytics modules. For example, using a Suspicious Domains module, an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

There are two types of preconfigured Suspicious Domains modules available in NetWitness Platform: Command and Control (C2) for Packets and C2 for Logs. The Suspicious Domains module defines a subset of events and the activities executed on those events for identifying suspicious C2 domains.

Before you deploy an ESA Analytics module for Automated Threat Detection, it is important to note that there are many potential installation configurations that may be installed on the ESA, including: ESA Analytics, ESA Correlation Rules, and the Context Hub. Each of these may take up resources, so it is important to consider sizing before deploying Automated Threat Detection on your ESA.

Prerequisites

- If you are using Packet data, you must have configured a Decoder for HTTP packet data, and you must have configured an HTTP Lua or Flex parser.
- If you are using web proxy log data, you must have configured the appropriate Log Decoder with the correct parser for your web proxy.
- If you are using web proxy log data, you must have updated to the latest log parsers. The following parsers are supported: Blue Coat Cache Flow (cacheflowelff), Cisco IronPort WSA (ciscoiportwsa), and Zscaler (zscalernss).
- If you are using web proxy log data, for best results you should configure all web proxies the same way (set to the same time zone, use the same collection method -syslog or batch, and if you use batch use the same batching cadence).
- A connection from the ESA host to the Whois service (same location as RSA Live cms:netwitness.com:443) must be opened on port 443. Verify with your System Administrator that this is complete.
- To whitelist a domain, you need to enable the Context Hub service.

IMPORTANT: Automated Threat Detection requires a "warm-up" period that acclimates the scoring algorithm to the traffic in your network. You should plan to configure Automated Threat Detection so that the warm-up period can run during normal traffic. For example, starting Automated Threat Detection on a Tuesday at 8:00 am in the timezone that contains the majority of your users allows the module to accurately analyze a day of normal traffic.

Configure Automated Threat Detection for Suspicious Domains

This procedure provides the steps needed to configure an ESA analytics Suspicious Domains module for Automated Threat Detection. ESA analytics modules, such as Suspicious Domains, are considered preconfigured because you do not have to manually create ESA rules for them.

The basic steps required are:

1. **Configure Log settings (for Logs only)**. Before you can use Automated Threat Detection for Logs, you must configure several settings. Skip this step if you plan to use Automated Threat Detection for Packets.
2. **Create a whitelist (optional) using the Context Hub service**. Creating a whitelist allows you to ensure that commonly accessed websites are excluded from any Automated Threat Detection scoring.
3. **Configure the Whois Lookup service**. The Whois service enables you to get accurate data about domains that you connect to. In order to ensure effective scoring, it is important that you configure the Whois Lookup service. Verify that the Whois Service is reachable from your environment.
4. **Map data sources to ESA Analytics modules**. You define how NetWitness Platform Automated Threat Detection should automatically detect advanced threats by mapping a preconfigured ESA analytics module to multiple data sources, such as Concentrators, and an ESA analytics service.
5. **Verify that the C2 incident rule is enabled and monitor for activity**. After mapping your Suspicous Domains module, a period of time is required for the scoring algorithm to warm-up. After the warm-up period, verify that the C2 rule is enabled in the Incident Rules and monitor to see if the rule is triggered.
6. **Verify that the incident rules are configured correctly**. When you view incidents in the Respond view, it is helpful if the incidents are grouped by Suspected C&C.

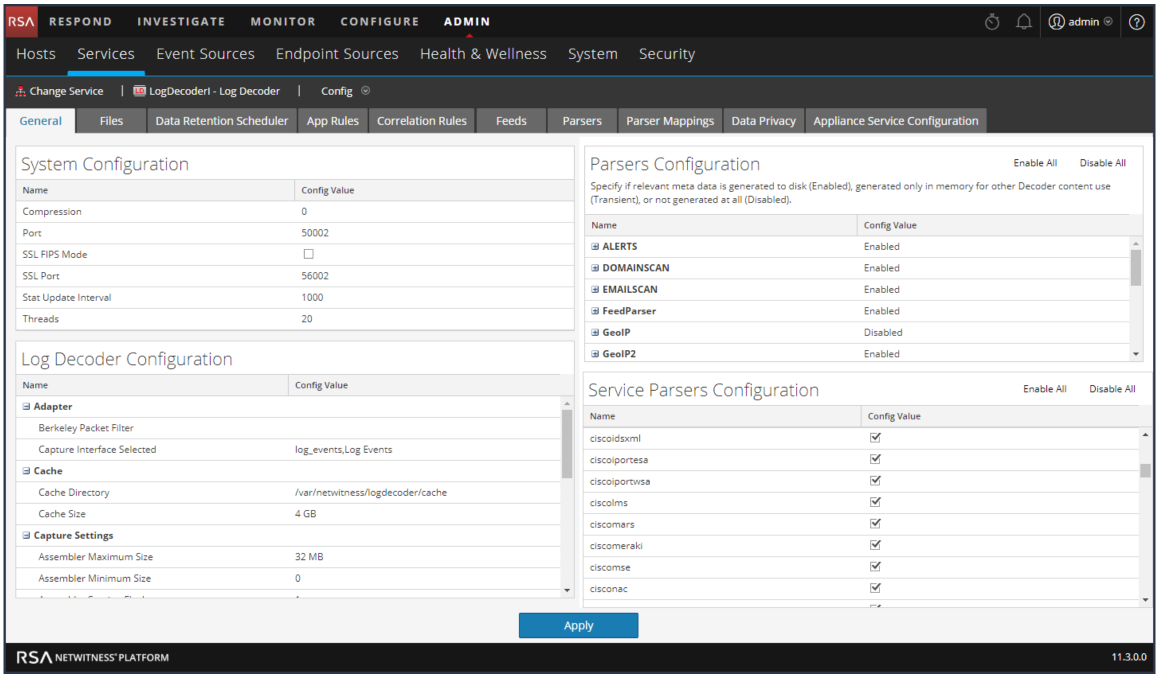
Step 1: (For Logs Only) Configure Log Settings

To configure Automated Threat Detection for Logs, you need to complete a few extra configuration steps:

- Verify that the supported parsers are enabled for your Log Decoder.
- Get the latest versions of the appropriate web proxy parser from RSA Live.
- Update the mapping on the Envision config file. This file is required to update the Log Decoder to work with the new meta available via the parsers.
- Verify that the table-map.xml file was updated correctly.
- Verify that the indexes were updated correctly.

To verify that your parsers are running on your Log Decoder:

1. Go to **ADMIN** > **Services**.
2. Select your Log Decoder and select > **View** > **Config**.
   The Service Parsers Configuration section shows a list of enabled parsers.
3. Verify that the appropriate web proxy parser is enabled.



System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ **Adapter**	
Berkeley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ **Cache**	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB
⊟ **Capture Settings**	
Assembler Maximum Size	32 MB
Assembler Minimum Size	0

Parsers Configuration

Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).

Name	Config Value
⊞ **ALERTS**	Enabled
⊞ **DOMAINSCAN**	Enabled
⊞ **EMAILSCAN**	Enabled
⊞ **FeedParser**	Enabled
⊞ **GeoIP**	Disabled
⊞ **GeoIP2**	Enabled

Service Parsers Configuration

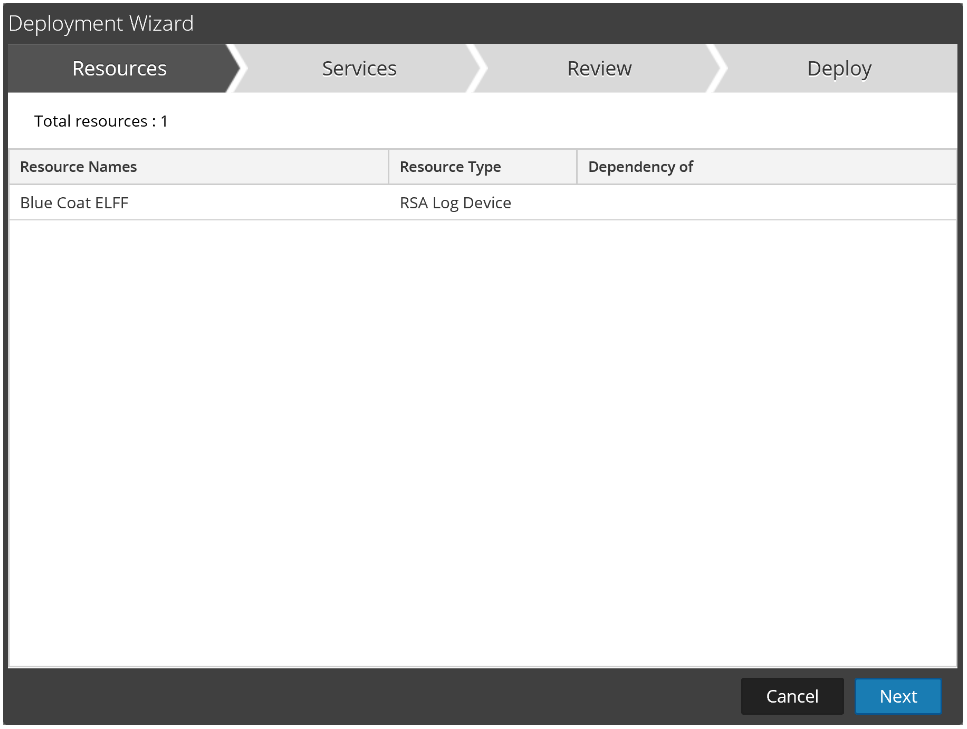
Name	Config Value
ciscoidsxml	☑
ciscoiportesa	☑
ciscoiportwsa	☑
ciscolms	☑
ciscomars	☑
ciscomeraki	☑
ciscomse	☑
cisconac	☑

To get the latest parsers from RSA Live:

1. Go to **CONFIGURE > Live Content**.
2. Enter a search term for one of the supported web proxy parsers.
3. Select the appropriate web proxy parser [for example, the Blue Coat ELFF (cacheflowelff) parser].

   Note: You should have taken steps to configure logging to occur on your web proxy parser correctly.

4. Click **Deploy**.
   The Deployment Wizard opens.



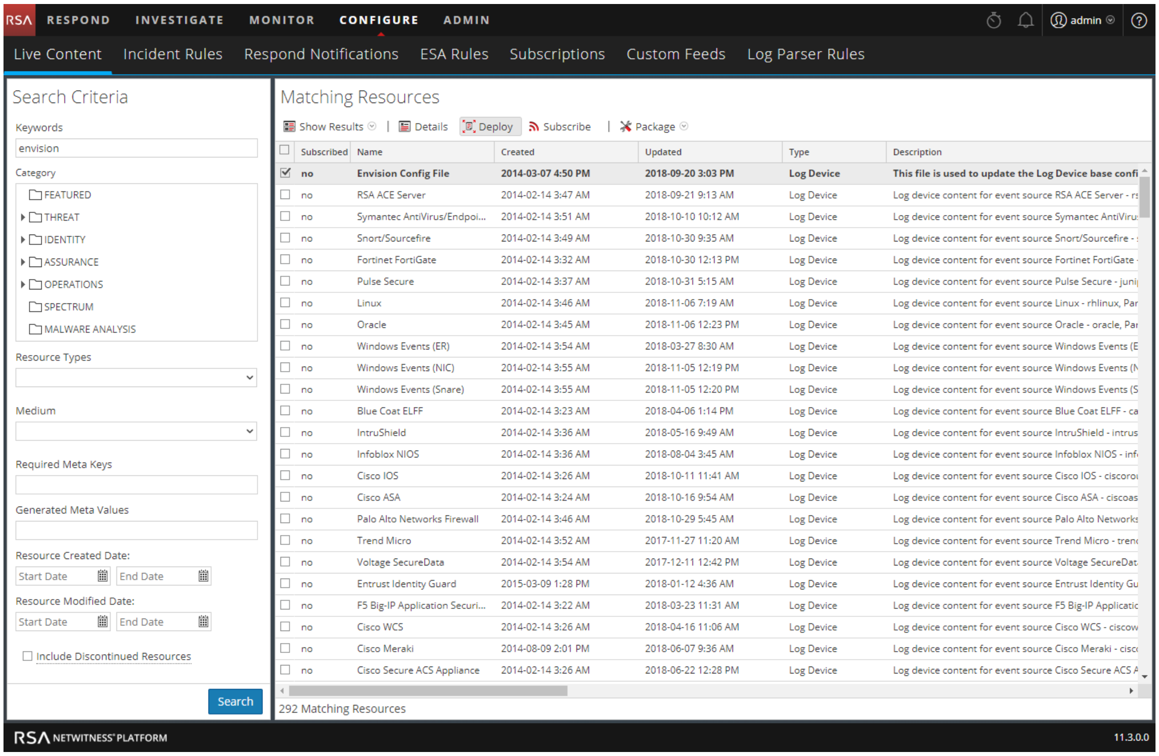
Total resources : 1

Resource Names	Resource Type	Dependency of
Blue Coat ELFF	RSA Log Device	

5. Click **Next** and under **Services**, select the Log Decoder as the Service.
6. Click **Next** and review your selection.
7. Click **Deploy** to deploy the parser to your Log Decoder.

To get the latest Envision Config file:

1. Go to **CONFIGURE** > **Live Content**.
2. Enter **envision** as the key word for the search.
3. Select the latest Envision Config File and click **Deploy**.



Keywords: envision

□ Include Discontinued Resources

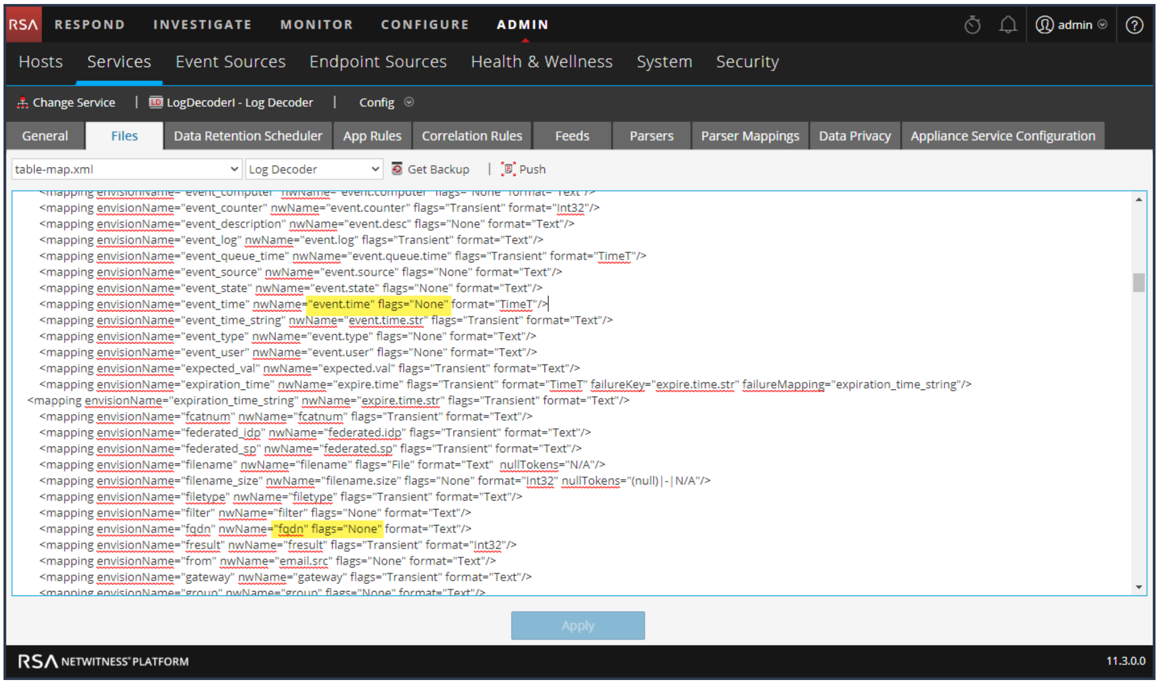
	Subscribed	Name	Created	Updated	Type	Description
☑	**no**	**Envision Config File**	**2014-03-07 4:50 PM**	**2018-09-20 3:03 PM**	**Log Device**	**This file is used to update the Log Device base confi**
□	no	RSA ACE Server	2014-02-14 3:47 AM	2018-09-21 9:13 AM	Log Device	Log device content for event source RSA ACE Server - rs
□	no	Symantec AntiVirus/Endpoi...	2014-02-14 3:51 AM	2018-10-10 10:12 AM	Log Device	Log device content for event source Symantec AntiViru
□	no	Snort/Sourcefire	2014-02-14 3:49 AM	2018-10-30 9:35 AM	Log Device	Log device content for event source Snort/Sourcefire -
□	no	Fortinet FortiGate	2014-02-14 3:32 AM	2018-10-30 12:13 PM	Log Device	Log device content for event source Fortinet FortiGate
□	no	Pulse Secure	2014-02-14 3:37 AM	2018-10-31 5:15 AM	Log Device	Log device content for event source Pulse Secure - juni
□	no	Linux	2014-02-14 3:46 AM	2018-11-06 7:19 AM	Log Device	Log device content for event source Linux - rhlinux, Par
□	no	Oracle	2014-02-14 3:45 AM	2018-11-06 12:23 PM	Log Device	Log device content for event source Oracle - oracle, Par
□	no	Windows Events (ER)	2014-02-14 3:54 AM	2018-03-27 8:30 AM	Log Device	Log device content for event source Windows Events (E
□	no	Windows Events (NIC)	2014-02-14 3:55 AM	2018-11-05 12:19 PM	Log Device	Log device content for event source Windows Events (N
□	no	Windows Events (Snare)	2014-02-14 3:55 AM	2018-11-05 12:20 PM	Log Device	Log device content for event source Windows Events (S
□	no	Blue Coat ELFF	2014-02-14 3:23 AM	2018-04-06 1:14 PM	Log Device	Log device content for event source Blue Coat ELFF - ca
□	no	IntruShield	2014-02-14 3:36 AM	2018-05-16 9:49 AM	Log Device	Log device content for event source IntruShield - intrus
□	no	Infoblox NIOS	2014-02-14 3:36 AM	2018-08-04 3:45 AM	Log Device	Log device content for event source Infoblox NIOS - inf
□	no	Cisco IOS	2014-02-14 3:26 AM	2018-10-11 11:41 AM	Log Device	Log device content for event source Cisco IOS - ciscoro
□	no	Cisco ASA	2014-02-14 3:24 AM	2018-10-16 9:54 AM	Log Device	Log device content for event source Cisco ASA - ciscoas
□	no	Palo Alto Networks Firewall	2014-02-14 3:46 AM	2018-10-29 5:45 AM	Log Device	Log device content for event source Palo Alto Networks
□	no	Trend Micro	2014-02-14 3:52 AM	2017-11-27 11:20 AM	Log Device	Log device content for event source Trend Micro - tren
□	no	Voltage SecureData	2014-02-14 3:54 AM	2017-12-11 12:42 PM	Log Device	Log device content for event source Voltage SecureDat
□	no	Entrust Identity Guard	2015-03-09 1:28 PM	2018-01-12 4:36 AM	Log Device	Log device content for event source Entrust Identity Gu
□	no	F5 Big-IP Application Securi...	2014-02-14 3:22 AM	2018-03-23 11:31 AM	Log Device	Log device content for event source F5 Big-IP Applicatio
□	no	Cisco WCS	2014-02-14 3:26 AM	2018-04-16 11:06 AM	Log Device	Log device content for event source Cisco WCS - ciscow
□	no	Cisco Meraki	2014-08-09 2:01 PM	2018-06-07 9:36 AM	Log Device	Log device content for event source Cisco Meraki - cisc
□	no	Cisco Secure ACS Appliance	2014-02-14 3:26 AM	2018-06-22 12:28 PM	Log Device	Log device content for event source Cisco Secure ACS A

292 Matching Resources

4. Click **Next**, and in the Deployment Wizard, under **Services**, select your Log Decoder.
5. Click **Next** and review your selection.
6. Click **Deploy** to deploy the Envision configuration file to the Log Decoder.

To verify that the Envision Configuration file was updated correctly:

1. Go to **ADMIN** > **Services**, select the Log Decoder, and then select ⚙ ⌄ > **View** > **Config** > **Files** tab.
2. Select the `table-map.xml` file. This file is modified when you update the Envision Configuration file.
3. Search for the term, *event.time*. The field should now read, *"event.time" flags ="None"*. This means that the event.time meta is now included in the mapping. Similarly, the fqdn flag should be set to "None".



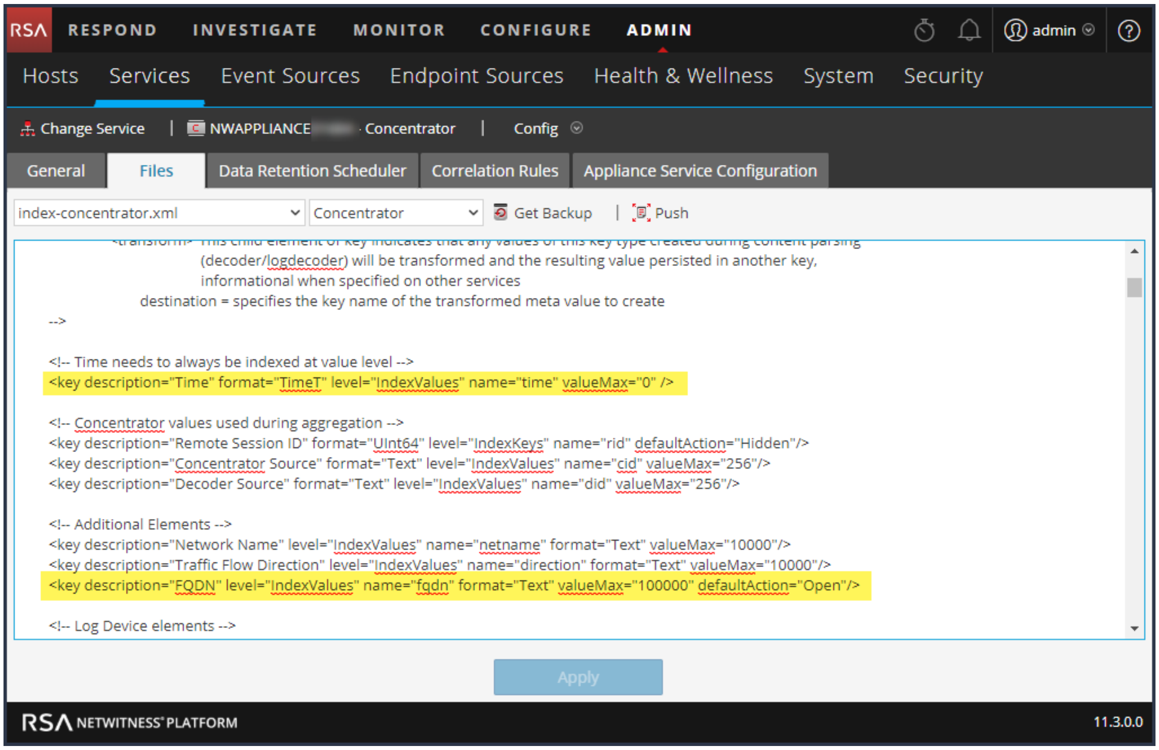
```
    <mapping envisionName="event_computer" nwName="event.computer" flags="None" format="Text"/>
    <mapping envisionName="event_counter" nwName="event.counter" flags="Transient" format="Int32"/>
    <mapping envisionName="event_description" nwName="event.desc" flags="None" format="Text"/>
    <mapping envisionName="event_log" nwName="event.log" flags="Transient" format="Text"/>
    <mapping envisionName="event_queue_time" nwName="event.queue.time" flags="Transient" format="TimeT"/>
    <mapping envisionName="event_source" nwName="event.source" flags="None" format="Text"/>
    <mapping envisionName="event_state" nwName="event.state" flags="None" format="Text"/>
    <mapping envisionName="event_time" nwName="event.time" flags="None" format="TimeT"/>
    <mapping envisionName="event_time_string" nwName="event.time.str" flags="Transient" format="Text"/>
    <mapping envisionName="event_type" nwName="event.type" flags="None" format="Text"/>
    <mapping envisionName="event_user" nwName="event.user" flags="None" format="Text"/>
    <mapping envisionName="expected_val" nwName="expected.val" flags="Transient" format="Text"/>
    <mapping envisionName="expiration_time" nwName="expire.time" flags="Transient" format="TimeT" failureKey="expire.time.str" failureMapping="expiration_time_string"/>
  <mapping envisionName="expiration_time_string" nwName="expire.time.str" flags="Transient" format="Text"/>
    <mapping envisionName="fcatnum" nwName="fcatnum" flags="Transient" format="Text"/>
    <mapping envisionName="federated_idp" nwName="federated.idp" flags="Transient" format="Text"/>
    <mapping envisionName="federated_sp" nwName="federated.sp" flags="Transient" format="Text"/>
    <mapping envisionName="filename" nwName="filename" flags="File" format="Text"  nullTokens="N/A"/>
    <mapping envisionName="filename_size" nwName="filename.size" flags="None" format="Int32" nullTokens="(null)|-|N/A"/>
    <mapping envisionName="filetype" nwName="filetype" flags="Transient" format="Text"/>
    <mapping envisionName="filter" nwName="filter" flags="None" format="Text"/>
    <mapping envisionName="fqdn" nwName="fqdn" flags="None" format="Text"/>
    <mapping envisionName="fresult" nwName="fresult" flags="Transient" format="Int32"/>
    <mapping envisionName="from" nwName="email.src" flags="None" format="Text"/>
    <mapping envisionName="gateway" nwName="gateway" flags="Transient" format="Text"/>
    <mapping envisionName="group" nwName="group" flags="None" format="Text"/>
```

To verify that the Indices for the index-concentrator.xml file are updated:

You must verify that the `index-concentrator.xml` file includes both the `event.time` and `fqdn` meta.

1. Go to **ADMIN** > **Services**, select your Concentrator, and then select ⚙ ⌄ > **View** > **Config**.
2. On the **Files** tab, select the `index-concentrator.xml` file.
3. Verify that the following entry exists in your `index-concentrator.xml` file. If not, ensure that your Concentrator is upgraded to the correct version:

```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text"
valueMax="100000" defaultAction="Open"/><key description="Event Time"
format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```



```
             <transform> This child element of key indicates that any values of this key type created during content parsing
                      (decoder/logdecoder) will be transformed and the resulting value persisted in another key,
                      informational when specified on other services
         destination = specifies the key name of the transformed meta value to create
-->

<!-- Time needs to always be indexed at value level -->
<key description="Time" format="TimeT" level="IndexValues" name="time" valueMax="0" />

<!-- Concentrator values used during aggregation -->
<key description="Remote Session ID" format="UInt64" level="IndexKeys" name="rid" defaultAction="Hidden"/>
<key description="Concentrator Source" format="Text" level="IndexValues" name="cid" valueMax="256"/>
<key description="Decoder Source" format="Text" level="IndexValues" name="did" valueMax="256"/>

<!-- Additional Elements -->
<key description="Network Name" level="IndexValues" name="netname" format="Text" valueMax="10000"/>
<key description="Traffic Flow Direction" level="IndexValues" name="direction" format="Text" valueMax="10000"/>
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/>

<!-- Log Device elements -->
```

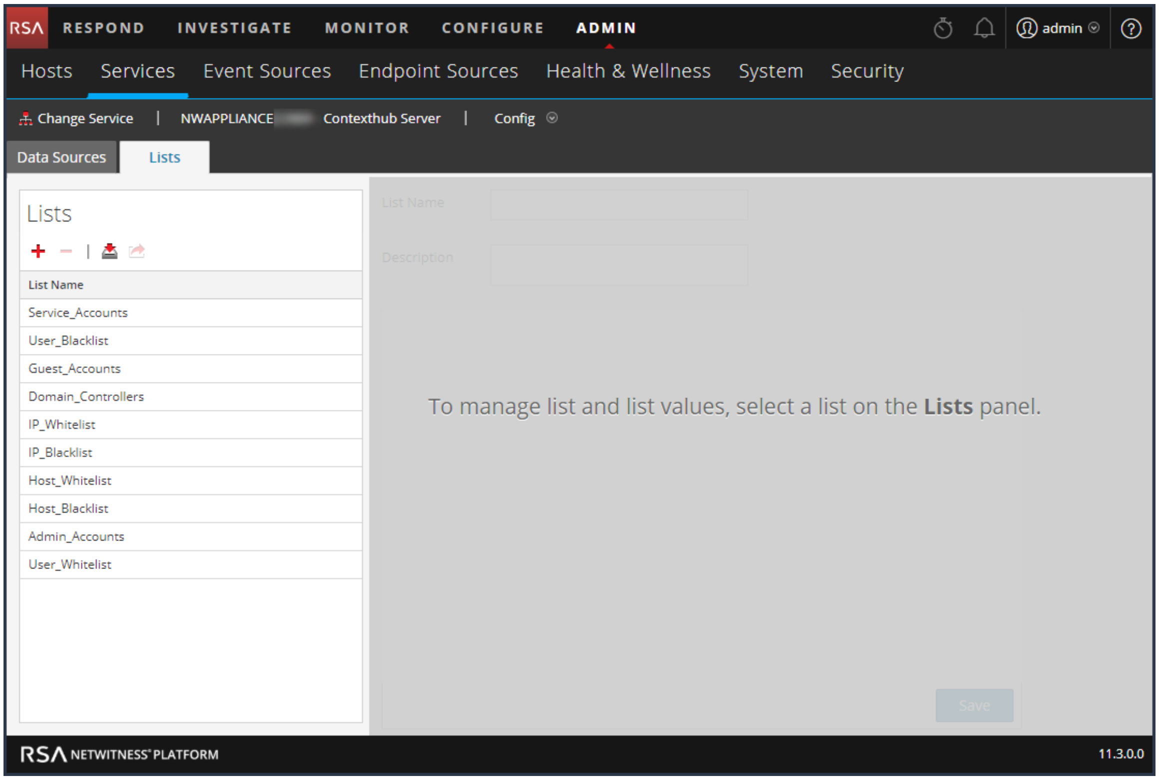
Step 2: Create a Domains Whitelist (Optional)

This procedure is used when working with Automated Threat Detection to ensure that certain domains do not trigger a threat score. Sometimes, a domain you access regularly may trigger an Automated Threat Detection score. For example, a weather service might have similar beaconing behavior as a Command and Control communication and trigger an unwarranted negative score. When this happens, it is called a false positive. To prevent triggering a false positive with a specific domain, you can add the domain to a whitelist. Most domains do not need to be whitelisted because the solution only alerts on very suspect behaviors. The domains you may want to whitelist are valid automated services that do not have many host connections.

> **Note:** For migrations from 10.6.x, if your previous Automated Threat Detection whitelist (Whitelisted Domains) appears on the Lists tab, you can rename it to **domains_whitelist** to use it for the Suspicious Domains modules.

1. Create a whitelist for domains in Context Hub named `domains_whitelist`:

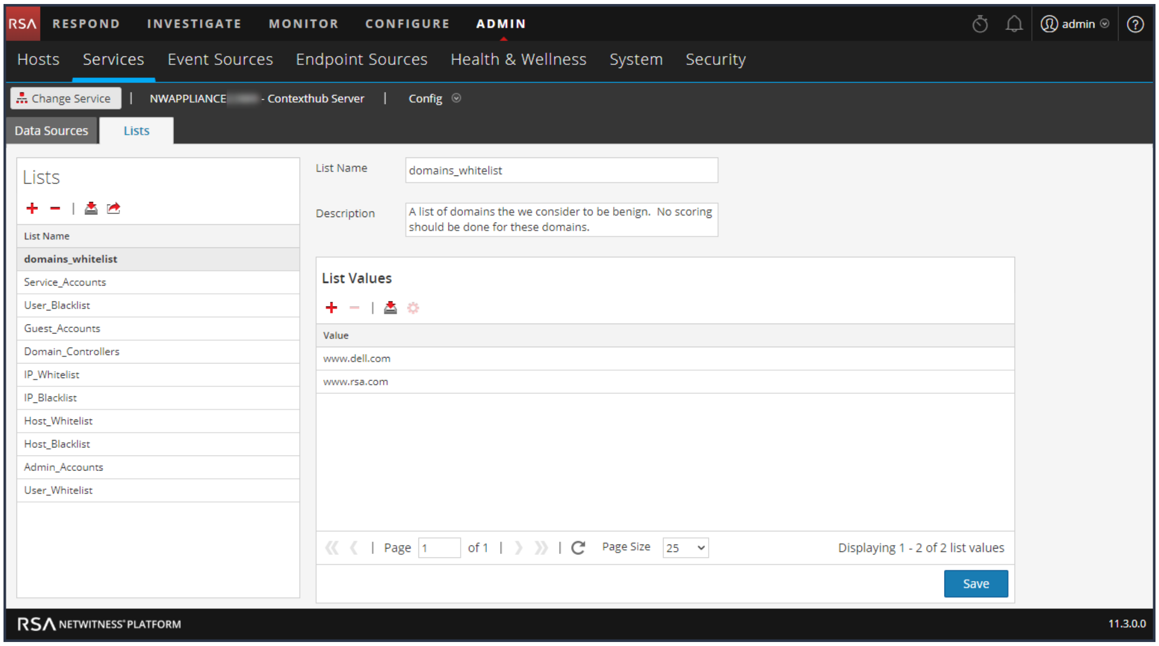
   a. Go to **ADMIN** > **Services**, select the Context Hub Server service, and then select ⚙ ⌄ > **View** > **Config** > **Lists** tab.
   The Lists tab shows the current lists in the Context Hub.



List Name
Service_Accounts
User_Blacklist
Guest_Accounts
Domain_Controllers
IP_Whitelist
IP_Blacklist
Host_Whitelist
Host_Blacklist
Admin_Accounts
User_Whitelist

To manage list and list values, select a list on the **Lists** panel.

b. In the Lists panel, click + to add a list. In the **List Name** field, type **`domains_whitelist`**. You must use this name in order for the module to recognize it.



List Name
domains_whitelist
Service_Accounts
User_Blacklist
Guest_Accounts
Domain_Controllers
IP_Whitelist
IP_Blacklist
Host_Whitelist
Host_Blacklist
Admin_Accounts
User_Whitelist

List Name: domains_whitelist

Description: A list of domains the we consider to be benign. No scoring should be done for these domains.

List Values

Value
www.dell.com
www.rsa.com

Displaying 1 - 2 of 2 list values

2. Manually add domains to the list or import a .CSV file containing a list of domains.
   You can enter full domains, or you can use a wild card to include all sub-domains for a given domain. For example, you can enter *.gov to whitelist all government IP addresses. However, you cannot use other regex functions, such as [a-z]*.gov. This is because using *.gov replaces an entire

string, such as www.irs.gov.

   a. To add domains manually, in the **List Values** section, click + to add domains.

   b. To remove a domain, select the domain and click − .

   c. To import a .CSV file, in the **List Values** section, click 📥, and in the **Import List Values** dialog, navigate to the .CSV file. Choose from the following delimiters: Comma, LF (Line Feed), and CR (Carriage Return) depending on how you have separated the values in your file. Click **Upload**.

3. Click **Save**.
   The **domains_whitelist** appears in the Lists panel. Analysts can add to this list from the Respond view and the Investigate view. The *Context Hub Configuration Guide* provides additional information.

Step 3: Configure the Whois Lookup Service

See "Configure Whois Lookup Service" in the *ESA Confguration Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Step 4: Map Data Sources to ESA Analytics Modules

See "Mapping ESA Data Sources to Analytics Modules" in the *ESA Confguration Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

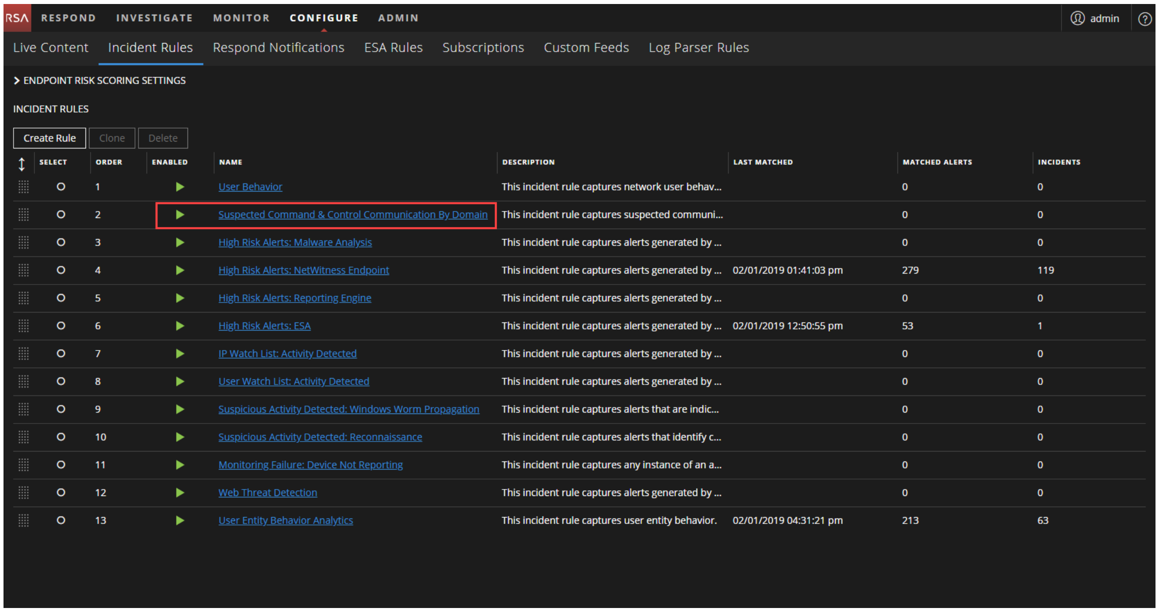
Step 5: Verify that the Suspected Command & Control By Domain Rule is Enabled and Monitor the Rule

Note: The information in this procedure applies to version 11.1 and later.

Verify and monitor the Suspected Command & Command Control by Domain rule in the Incident Rules list.

1. Go to **CONFIGURE > Incident Rules**.

2. In the Incident Rules list, locate the **Suspected Command & Control Communication by Domain** rule and verify that it displays a green Enabled icon (▶) next to the rule name.



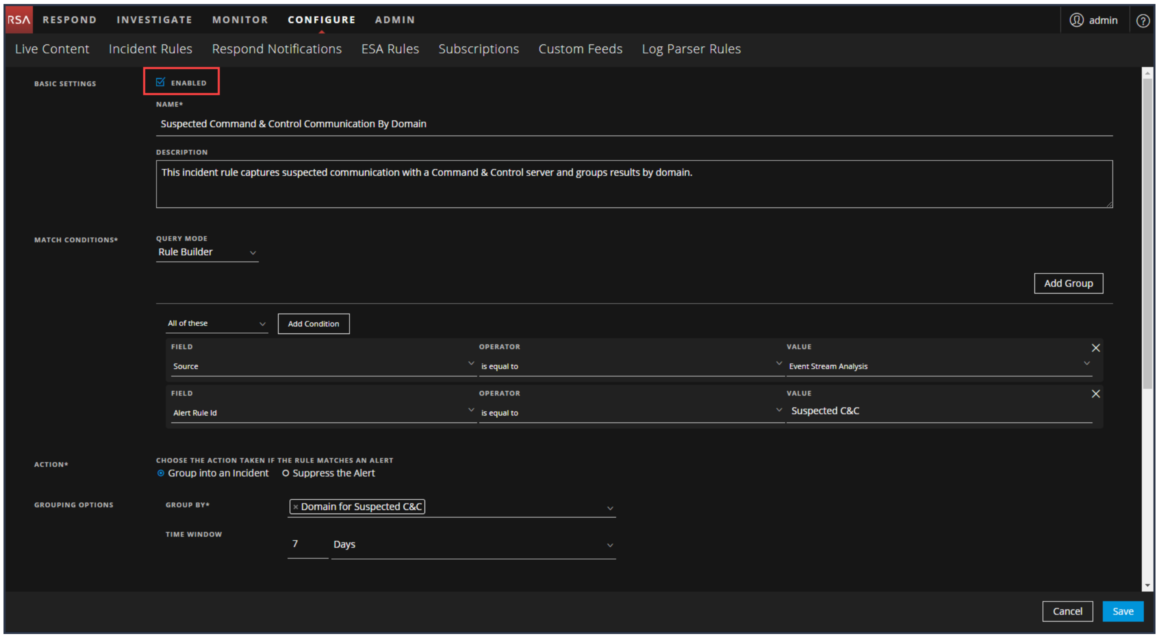
INCIDENT RULES

SELECT	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS
○	1	▶	User Behavior	This incident rule captures network user behav...		0	0
○	2	▶	Suspected Command & Control Communication By Domain	This incident rule captures suspected communi...		0	0
○	3	▶	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by ...		0	0
○	4	▶	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by ...	02/01/2019 01:41:03 pm	279	119
○	5	▶	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by ...		0	0
○	6	▶	High Risk Alerts: ESA	This incident rule captures alerts generated by ...	02/01/2019 12:50:55 pm	53	1
○	7	▶	IP Watch List: Activity Detected	This incident rule captures alerts generated by ...		0	0
○	8	▶	User Watch List: Activity Detected	This incident rule captures alerts generated by ...		0	0
○	9	▶	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indic...		0	0
○	10	▶	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify c...		0	0
○	11	▶	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an a...		0	0
○	12	▶	Web Threat Detection	This incident rule captures alerts generated by ...		0	0
○	13	▶	User Entity Behavior Analytics	This incident rule captures user entity behavior.	02/01/2019 04:31:21 pm	213	63

3. If the rule is not enabled:

   a. Click the link in the NAME field to open it.

   b. In the Incident Rule Details view, select **Enabled** and click **Save**.



BASIC SETTINGS

☑ ENABLED

NAME*
Suspected Command & Control Communication By Domain

DESCRIPTION
This incident rule captures suspected communication with a Command & Control server and groups results by domain.

MATCH CONDITIONS*

QUERY MODE
Rule Builder

All of these

FIELD	OPERATOR	VALUE
Source	is equal to	Event Stream Analysis
Alert Rule Id	is equal to	Suspected C&C

ACTION*

CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT
● Group into an Incident ○ Suppress the Alert

GROUPING OPTIONS

GROUP BY*
× Domain for Suspected C&C

TIME WINDOW
7 Days

4. In the Incident Rules list, monitor the statistics in the following fields to see if the rule is triggered:

- **Last Matched**: Shows the time when an alert was successfully matched with the rule.
- **Matched Alerts**: Displays the number of alerts that matched the rule.
- **Incidents**: Displays the number of incidents created by the rule.

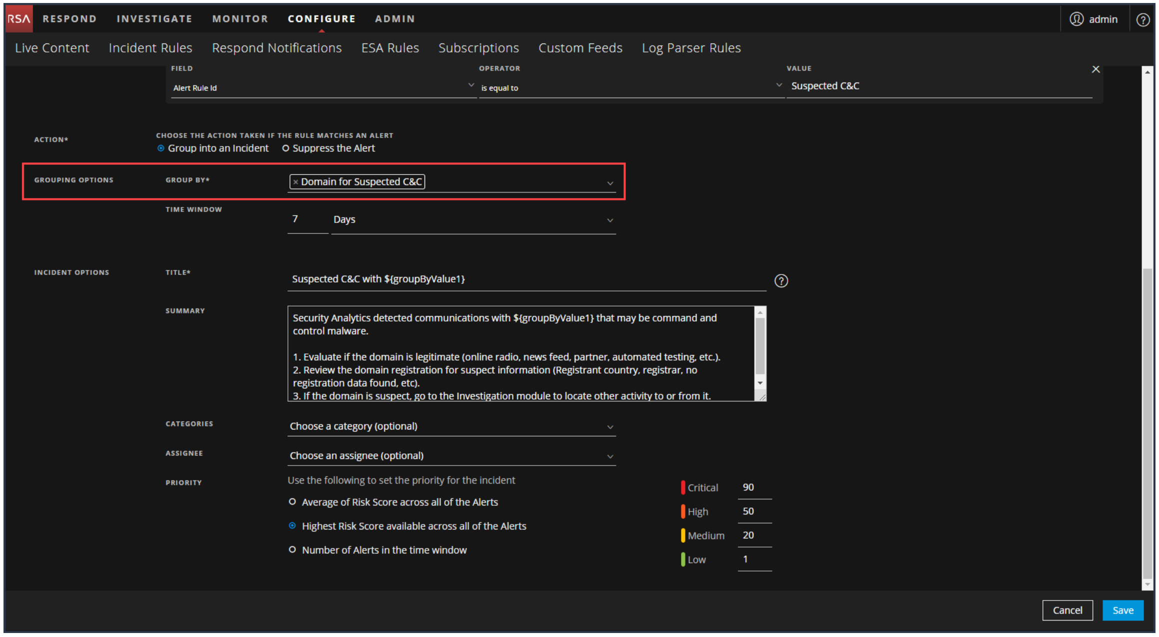
By default, these values reset to zero every 7 days. For more information, see "Set Counter for Matched Alerts and Incidents" in the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Step 6: Verify that the Incident is grouped by Suspected C&C

Note: The information in this procedure applies to version 11.1 and later.

In order to group incidents correctly in the Respond view, set the Group By condition to Domain for Suspected C&C.

1. Go to **CONFIGURE** > **Incident Rules**.
2. In the Incident Rules list, locate the **Suspected Command & Control Communication by Domain** rule and click the link in the NAME field to open it.
3. In Grouping Options section, verify that the **Group By** field is set to *Domain for Suspected C&C*.



FIELD: Alert Rule Id
OPERATOR: is equal to
VALUE: Suspected C&C

ACTION*
CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT
● Group into an Incident ○ Suppress the Alert

GROUPING OPTIONS
GROUP BY*: × Domain for Suspected C&C
TIME WINDOW: 7 Days

INCIDENT OPTIONS
TITLE*: Suspected C&C with ${groupByValue1}
SUMMARY:
Security Analytics detected communications with ${groupByValue1} that may be command and control malware.

1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.).
2. Review the domain registration for suspect information (Registrant country, registrar, no registration data found, etc).
3. If the domain is suspect, go to the Investigation module to locate other activity to or from it.

CATEGORIES: Choose a category (optional)
ASSIGNEE: Choose an assignee (optional)
PRIORITY
Use the following to set the priority for the incident
○ Average of Risk Score across all of the Alerts
● Highest Risk Score available across all of the Alerts
○ Number of Alerts in the time window

🟥 Critical	90
🟧 High	50
🟨 Medium	20
🟩 Low	1

This aggregates alerts and incidents are created for "Suspected C&C."

Result

After you deploy the ESA Analytics Suspicious Domains module mapping for Automated Threat Detection, your ESA begins to perform analytics on the HTTP traffic. You can view detailed information for each incident in the Respond view.

Next Steps

Monitor the Respond view to see if the rule is triggered. The *NetWitness Respond User Guide* provides additional information. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Troubleshooting Automated Threat Detection

NetWitness Platform Automated Threat Detection is an analytics engine that examines your HTTP data. It also makes use of other components, such as the Whois and Context Hub services, which can add complexity to your installation. This topic provides suggestions to help you find issues if your Automated Threat Detection deployment does not provide the results that you expect.

Possible Issues

Problem	Possible Causes	Solutions
I'm seeing too many alerts (false positives).	Several	One possible cause is that the Whois Lookup service is failing or is not configured. The Whois lookup is helpful in determining whether a URL is valid, and if the connection fails or is not properly configured, it can result in false positives. See "Configure Whois Lookup Service" in the *ESA Configuration Guide*.
		You may need to whitelist URLs. Sometimes the legitimate behavior for a URL triggers an alert. One way to prevent this from occurring is to add the URL to the whitelist. See "Add an Entity to a Whitelist" in the *NetWitness Respond User Guide*.
I'm not seeing any alerts.	The ESA host requires a "warm-up" period when you deploy an ESA Analytics Module Mapping for Automated Threat Detection.	When you deploy an ESA analytics module mapping for Automated Threat Detection, there is a "warm-up" period, during which no alerts are viewable. Each module type has a default warm-up period and you need to wait until the warm-up period is complete. For more information, see "Mapping ESA Data Sources to Analytics Modules" in the *ESA Configuration Guide*.
I'm seeing performance issues (more resource usage or a drop in throughput).	Several	If you are having performance issues on an ESA host that is running both Automated Threat Detection (ESA Analytics) and ESA rules, follow the troubleshooting steps for rules. For these troubleshooting steps, see "Troubleshoot ESA" in the *Alerting with ESA Correlation Rules User Guide*.

Problem	Possible Causes	Solutions
In NetWitness Platform 11.3, the Respond Event List in 11.3 does not show the Command and Control (C2) enrichment information for HTTP packet alerts in Suspected C&C Incidents.	In version 11.3, you can view the C2 enrichment information in the Alert Details view.	View C2 enrichment information for the Suspected C&C incidents in the corresponding alerts in the Alert Details view. 1. Go to **RESPOND > Incidents**, look for a **Suspected C&C** incident, and note the incident ID. 2. Go to **RESPOND > Alerts** and in the Filters panel, select the following to locate an alert in the Alerts list with the incident ID noted above: a. In **Alert Names** section, select **http-packet**. b. In the **Part of Incident** section, select **Yes**. If you are still not able to locate an alert in the Alerts list with the incident ID noted above, try filtering your alerts list more using the time range of the incident. 3. In the Alerts list, click the **http-packet** link in the **NAME** field of the alert associated with the incident ID. The Event Details view shows the C2 enrichment information.

Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.