NOZOMI
NETWORKS

Nozomi Networks QRadar App

User Manual

Table of Contents

Technical information

Product details

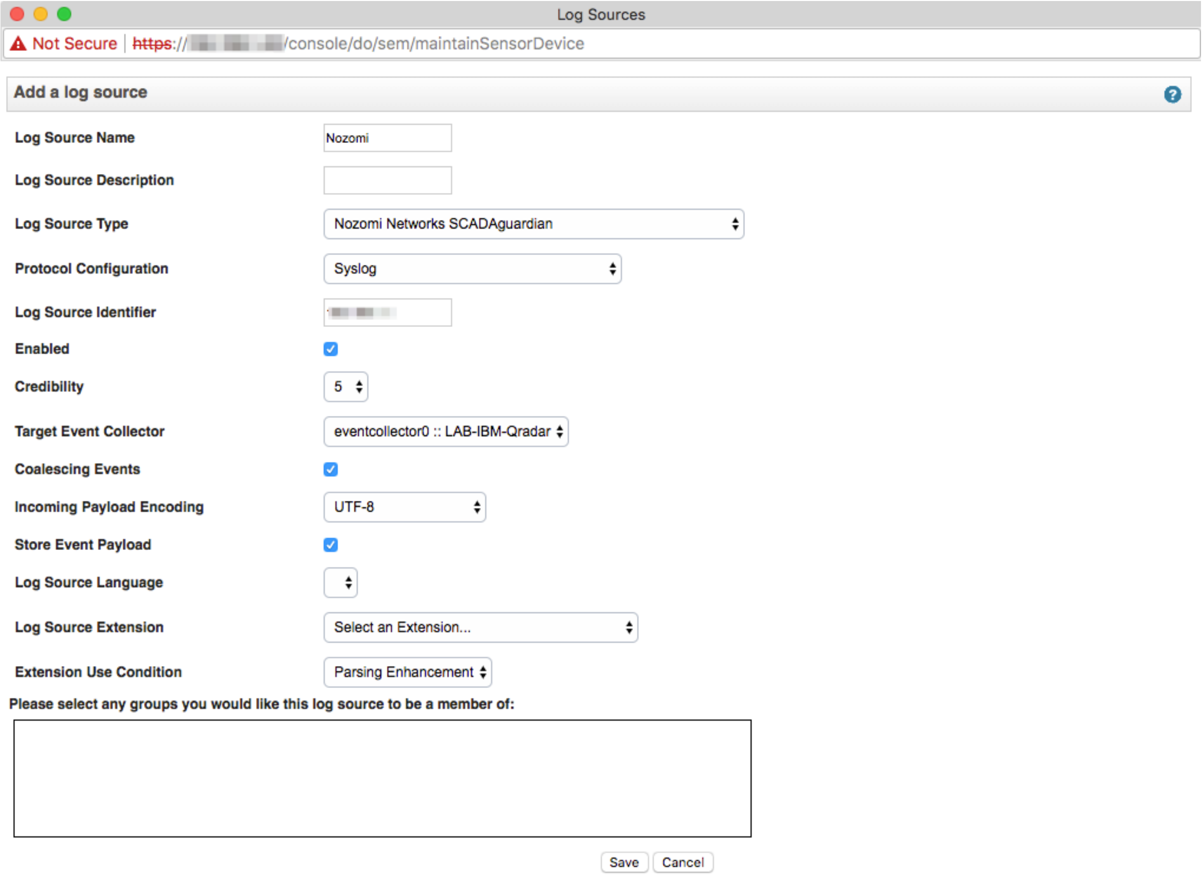
- version: 2.0.0
- release date: Oct 2019

Prerequisites

- minimum QRadar version: 7.3.0
- supported browsers: Firefox (verified on 59.0), Chrome (verified on 66.0), Internet Explorer (verified on 11.0)

Installation

1. download the extension from https://exchange.xforce.ibmcloud.com/hub/
2. in QRadar go to the Admin tab
3. click on Extensions Management
4. click on Add and upload the zip you downloaded using the extensions management console, overwrite any existing custom properties
5. add a new log source as per the screenshot below



Log Sources
Not Secure | ~~https~~://[redacted]/console/do/sem/maintainSensorDevice

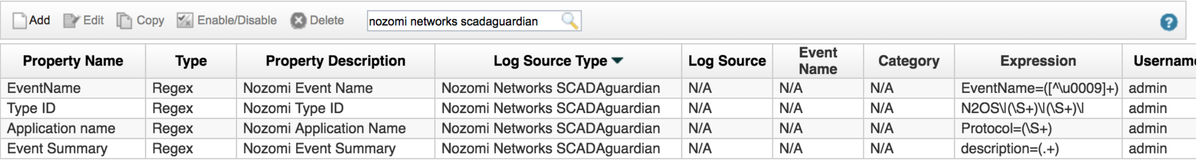
Add a log source

Log Source Name	Nozomi
Log Source Description	
Log Source Type	Nozomi Networks SCADAguardian
Protocol Configuration	Syslog
Log Source Identifier	[redacted]
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: LAB-IBM-Qradar
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑
Log Source Language	
Log Source Extension	Select an Extension...
Extension Use Condition	Parsing Enhancement

Please select any groups you would like this log source to be a member of:

Custom properties

The following screenshot highlights the custom properties that will be added to your Qradar installation.



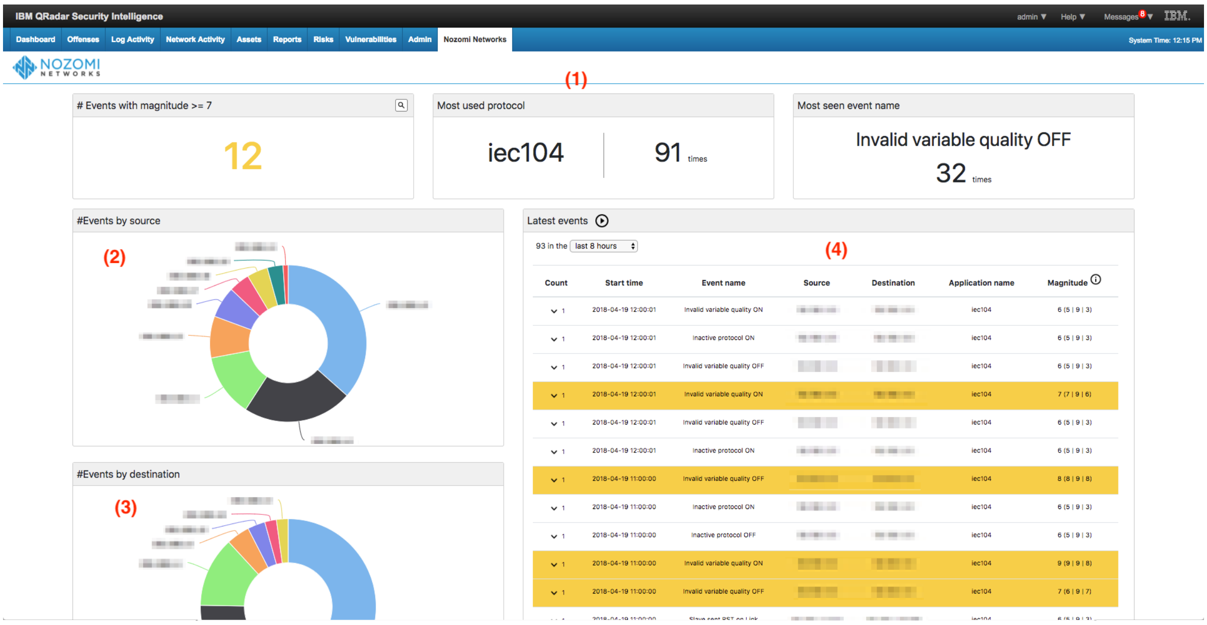
<table>
<tr><th>Property Name</th><th>Type</th><th>Property Description</th><th>Log Source Type</th><th>Log Source</th><th>Event Name</th><th>Category</th><th>Expression</th><th>Usernam</th></tr>
<tr><td>EventName</td><td>Regex</td><td>Nozomi Event Name</td><td>Nozomi Networks SCADAguardian</td><td>N/A</td><td>N/A</td><td>N/A</td><td>EventName=([^\u0009]+)</td><td>admin</td></tr>
<tr><td>Type ID</td><td>Regex</td><td>Nozomi Type ID</td><td>Nozomi Networks SCADAguardian</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N2OS\|(\S+)\|(\S+)\|</td><td>admin</td></tr>
<tr><td>Application name</td><td>Regex</td><td>Nozomi Application Name</td><td>Nozomi Networks SCADAguardian</td><td>N/A</td><td>N/A</td><td>N/A</td><td>Protocol=(\S+)</td><td>admin</td></tr>
<tr><td>Event Summary</td><td>Regex</td><td>Nozomi Event Summary</td><td>Nozomi Networks SCADAguardian</td><td>N/A</td><td>N/A</td><td>N/A</td><td>description=(.+)</td><td>admin</td></tr>
</table>

Overview

Nozomi Networks QRadar App helps you understand when a threat is happening and drill down to the possible causes with a couple clicks. By leveraging the simple user interface you will be able to understand what's going on with a simple glance.

With its live streaming dashboard Nozomi Networks QRadar App shows

- a header at the top (1)
- a pie chart containing events grouped by source (2)
- a pie chart containing events grouped by destination (3)
- events (limited to 5000) coming from Nozomi Networks Guardian, last records will appear at the top (4).



Events with magnitude >= 7

12

Most used protocol

iec104 | 91 times

Most seen event name

Invalid variable quality OFF

32 times

#Events by source

#Events by destination

Latest events

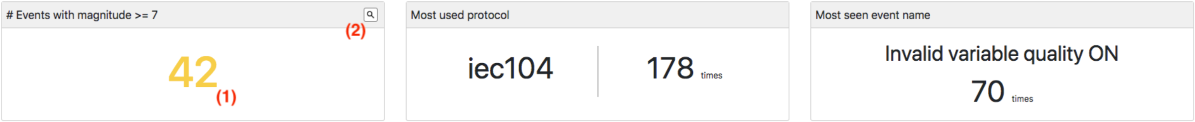
93 in the last 8 hours

Count	Start time	Event name	Source	Destination	Application name	Magnitude ⓘ
1	2018-04-19 12:00:01	Invalid variable quality ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 12:00:01	Inactive protocol ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 12:00:01	Invalid variable quality OFF	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 12:00:01	Invalid variable quality ON	[redacted]	[redacted]	iec104	7 (7 | 9 | 6)
1	2018-04-19 12:00:01	Invalid variable quality OFF	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 12:00:01	Inactive protocol ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 11:00:00	Invalid variable quality OFF	[redacted]	[redacted]	iec104	8 (8 | 9 | 8)
1	2018-04-19 11:00:00	Inactive protocol ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 11:00:00	Inactive protocol OFF	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
1	2018-04-19 11:00:00	Invalid variable quality ON	[redacted]	[redacted]	iec104	9 (9 | 9 | 8)
1	2018-04-19 11:00:00	Invalid variable quality OFF	[redacted]	[redacted]	iec104	7 (6 | 9 | 7)
1	2018-04-19 11:00:00	Slave sent RST on Link	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)

Header: important information at first glance

We've crafted the header with attention to the details that matter the most, you will be able to spot if there's a peak in a certain protocol usage, or if you are getting lots of troublesome events; here's what you'll find:

- number of events with a magnitude greater or equal than 7
- most used protocol along with the times it was seen
- most seen event name along with the times it was seen



Events with magnitude >= 7

42

Most used protocol

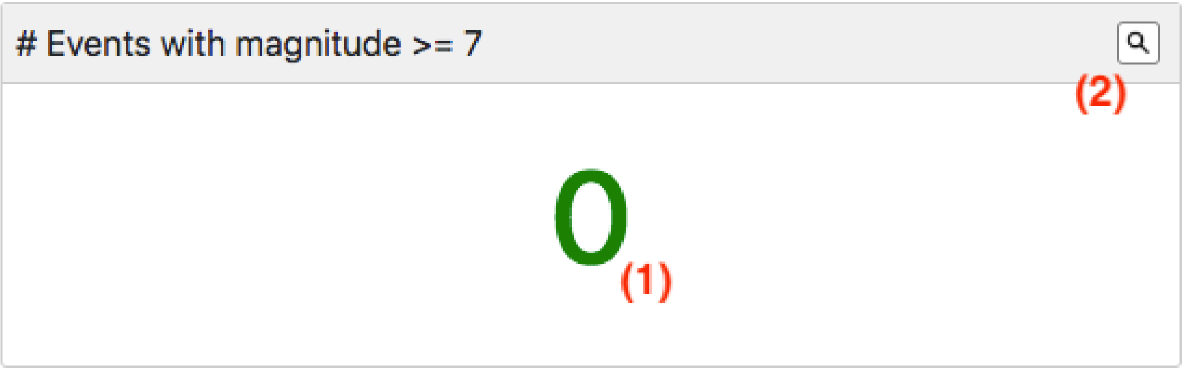
iec104 178 times

Most seen event name

Invalid variable quality ON

70 times

When events with magnitude greater or equal than 7 start appearing, the total (1) will turn to yellow; you can see those events by clicking on the magnifying lens (2).



Events with magnitude >= 7

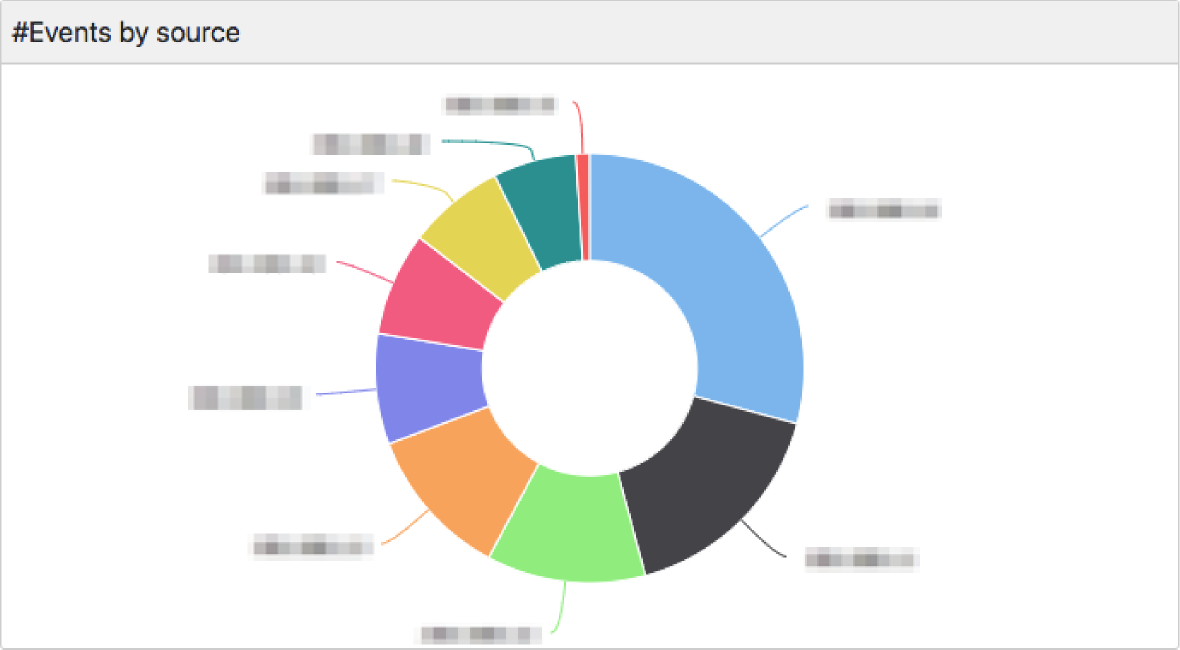
0

In detail

These widgets will help you drill down towards the problem.

Events by source

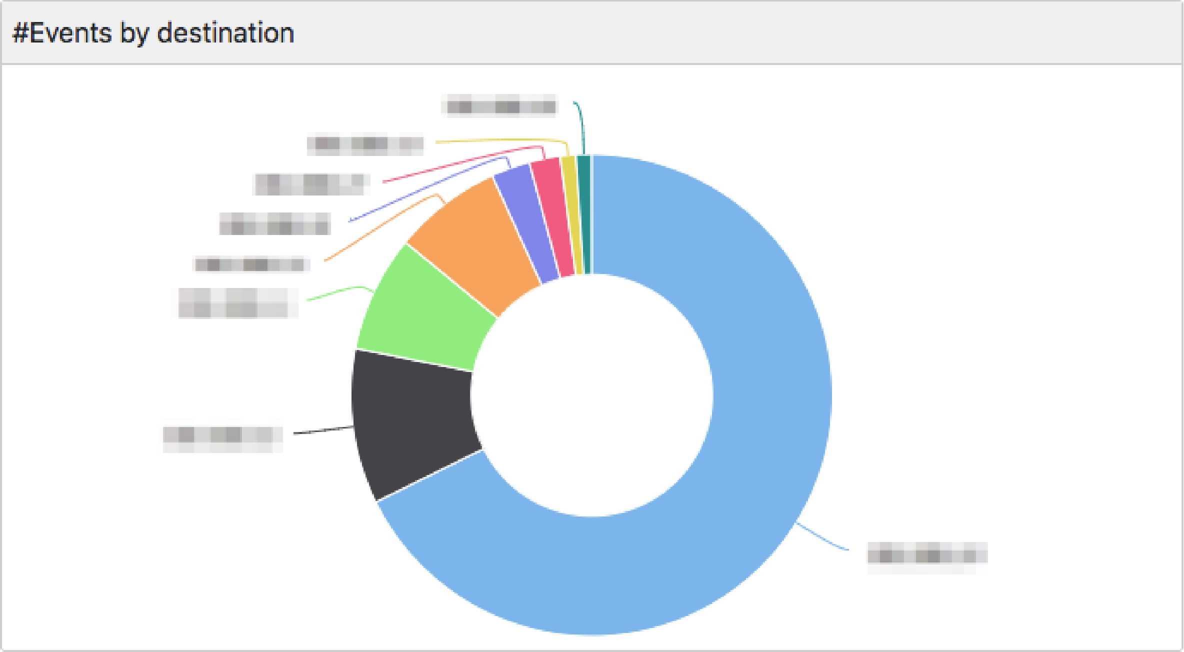
Events grouped by source IP. Click on a slice to filter events by that IP.



#Events by source

Events by destination

Events grouped by destination IP. Click on a slice to filter events by that IP.

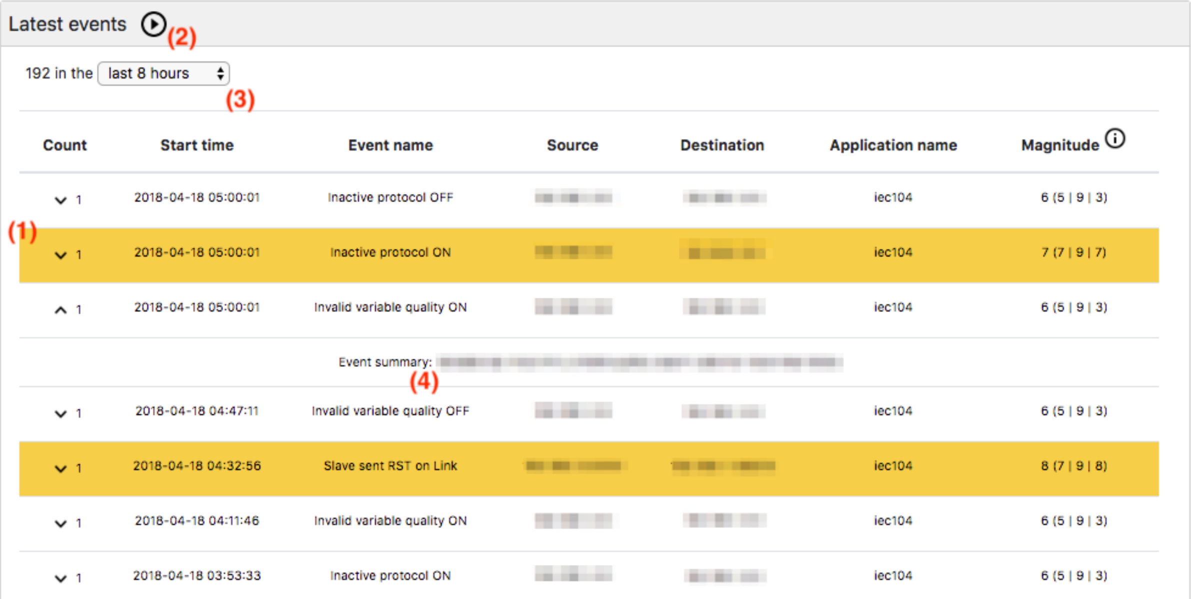


#Events by destination

Events list

These events are filtered to contain just those coming from Nozomi Networks Guardian, last events appear at the top. QRadar assigns to each event a magnitude, you will see it highlighted in yellow (1) if the magnitude is 7 or greater.

We're constantly updating the events coming into QRadar, however you can pause the stream of events by clicking on the pause / unpause button (2), this is particularly useful if you want to have a look at the event summary of the event (4) (click on an event to show it), or just calmly look at the list without it being refreshed. Press the button again to resume the stream. Click on the dropdown list (3) to define the time window for your events.



Latest events

192 in the last 8 hours

Count	Start time	Event name	Source	Destination	Application name	Magnitude
∨ 1	2018-04-18 05:00:01	Inactive protocol OFF	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
∨ 1	2018-04-18 05:00:01	Inactive protocol ON	[redacted]	[redacted]	iec104	7 (7 | 9 | 7)
∧ 1	2018-04-18 05:00:01	Invalid variable quality ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
		Event summary: [redacted]				
∨ 1	2018-04-18 04:47:11	Invalid variable quality OFF	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
∨ 1	2018-04-18 04:32:56	Slave sent RST on Link	[redacted]	[redacted]	iec104	8 (7 | 9 | 8)
∨ 1	2018-04-18 04:11:46	Invalid variable quality ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)
∨ 1	2018-04-18 03:53:33	Inactive protocol ON	[redacted]	[redacted]	iec104	6 (5 | 9 | 3)

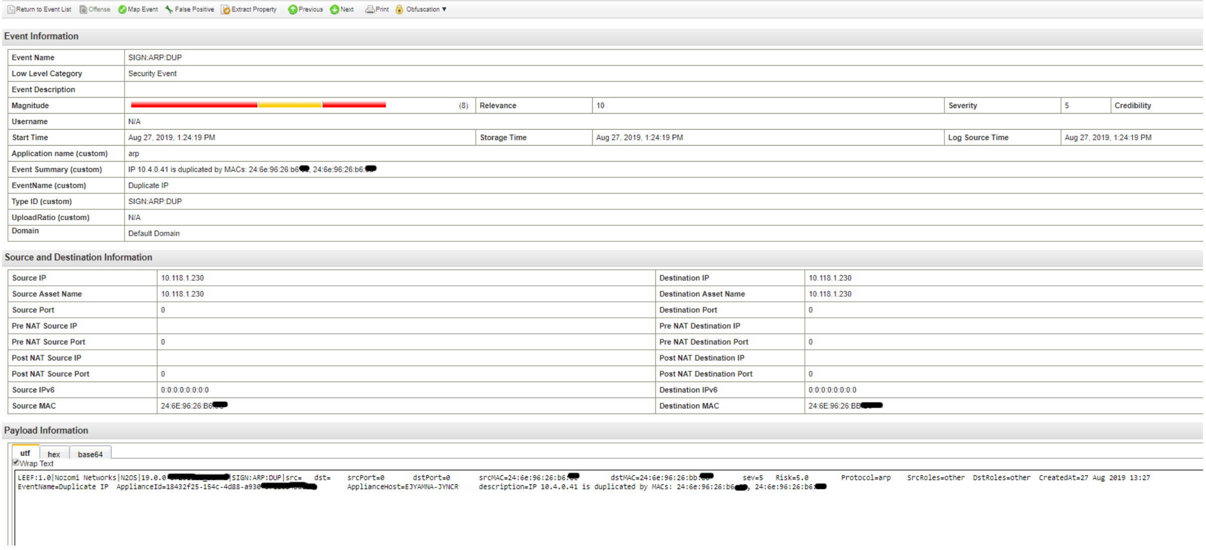
Events shown in this list will be limited to 5000

Events

Nozomi QRadar App send to QRadar events that can be alerts, assets or health-logs.

Some alerts events, for example duplicate ARP, are on layer two. It means that the source and destination have only MAC address.

QRadar in this case add as default IP the IP of the log_source, the Nozomi appliance sending data.



Event Information

Event Name	SIGN:ARP:DUP						
Low Level Category	Security Event						
Event Description							
Magnitude	(8)	Relevance	10	Severity	5	Credibility	
Username	N/A						
Start Time	Aug 27, 2019, 1:24:19 PM	Storage Time	Aug 27, 2019, 1:24:19 PM	Log Source Time	Aug 27, 2019, 1:24:19 PM		
Application name (custom)	arp						
Event Summary (custom)	IP 10.4.0.41 is duplicated by MACs: 24:6e:96:26:b6[redacted], 24:6e:96:26:b6:[redacted]						
EventName (custom)	Duplicate IP						
Type ID (custom)	SIGN:ARP:DUP						
UploadRatio (custom)	N/A						
Domain	Default Domain						

Source and Destination Information

Source IP	10.118.1.230	Destination IP	10.118.1.230
Source Asset Name	10.118.1.230	Destination Asset Name	10.118.1.230
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	24:6E:96:26:B6[redacted]	Destination MAC	24:6E:96:26:BB[redacted]

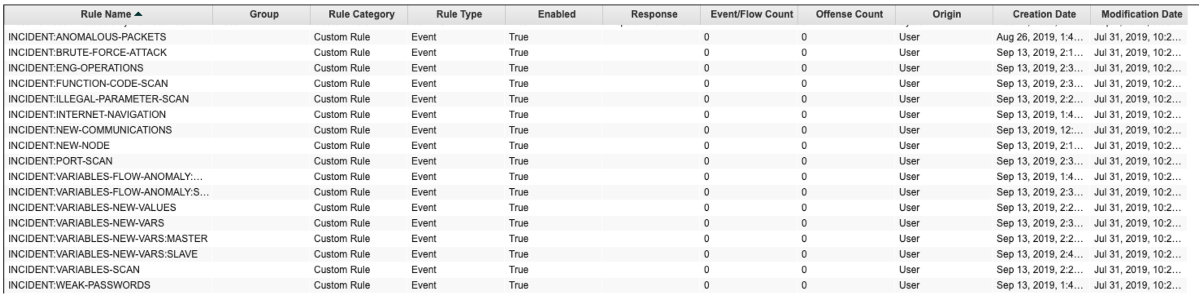
Payload Information

☑ Wrap Text

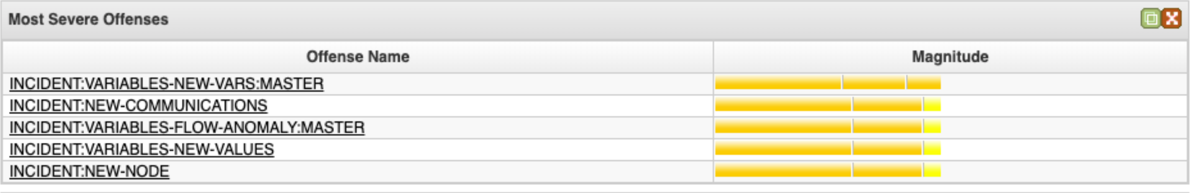
```
LEEF:1.0|Nozomi Networks|N2OS|19.0.0[redacted]|SIGN:ARP:DUP|src=   dst=     srcPort=0       dstPort=0       srcMAC=24:6e:96:26:b6:[redacted]       dstMAC=24:6e:96:26:bb:[redacted]       sev=5   Risk=5.0        Protocol=arp    SrcRoles=other  DstRoles=other  CreatedAt=27 Aug 2019 13:27
EventName=Duplicate IP  ApplianceId=18432f25-154c-4d88-a930[redacted]       ApplianceHost=EJYAMNA-JYNCR     description=IP 10.4.0.41 is duplicated by MACs: 24:6e:96:26:b6[redacted], 24:6e:96:26:b6:[redacted]
```

Rules

Nozomi QRadar App includes a set of rules that trigger offences in case some `incident events` are received.



Rule Name ▲	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
INCIDENT:ANOMALOUS-PACKETS		Custom Rule	Event	True		0	0	User	Aug 26, 2019, 1:4…	Jul 31, 2019, 10:2…
INCIDENT:BRUTE-FORCE-ATTACK		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:1…	Jul 31, 2019, 10:2…
INCIDENT:ENG-OPERATIONS		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:3…	Jul 31, 2019, 10:2…
INCIDENT:FUNCTION-CODE-SCAN		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:3…	Jul 31, 2019, 10:2…
INCIDENT:ILLEGAL-PARAMETER-SCAN		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:2…	Jul 31, 2019, 10:2…
INCIDENT:INTERNET-NAVIGATION		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 1:4…	Jul 31, 2019, 10:2…
INCIDENT:NEW-COMMUNICATIONS		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 12:…	Jul 31, 2019, 10:2…
INCIDENT:NEW-NODE		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:1…	Jul 31, 2019, 10:2…
INCIDENT:PORT-SCAN		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:3…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-FLOW-ANOMALY:…		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 1:4…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-FLOW-ANOMALY:S…		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:3…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-NEW-VALUES		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:2…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-NEW-VARS		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:3…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-NEW-VARS:MASTER		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:2…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-NEW-VARS:SLAVE		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:4…	Jul 31, 2019, 10:2…
INCIDENT:VARIABLES-SCAN		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 2:2…	Jul 31, 2019, 10:2…
INCIDENT:WEAK-PASSWORDS		Custom Rule	Event	True		0	0	User	Sep 13, 2019, 1:4…	Jul 31, 2019, 10:2…



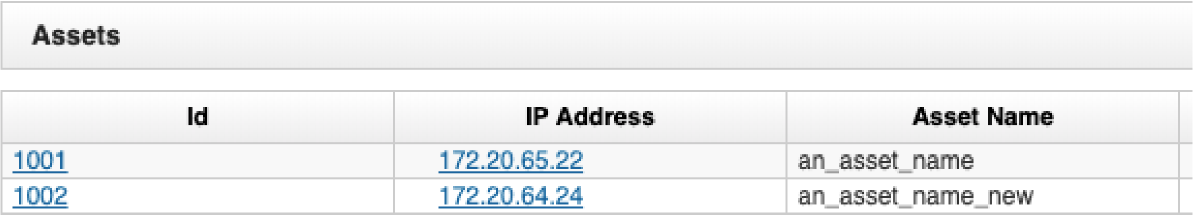
Most Severe Offenses

Offense Name	Magnitude
INCIDENT:VARIABLES-NEW-VARS:MASTER	
INCIDENT:NEW-COMMUNICATIONS	
INCIDENT:VARIABLES-FLOW-ANOMALY:MASTER	
INCIDENT:VARIABLES-NEW-VALUES	
INCIDENT:NEW-NODE	

Assets

Nozomi QRadar App inject through `asset info events` assets object into QRadar environment to improve your asset visibility.

Only from version 19.0.2, N2OS provides assets information to QRadar.



Assets

Id	IP Address	Asset Name
1001	172.20.65.22	an_asset_name
1002	172.20.64.24	an_asset_name_new

Troubleshooting

If you don't see any data in Nozomi Networks QRadar App make sure you are sending events to QRadar. You might also want to try and set the time window to a more recent value.

After an update of the Nozomi Networks QRadar App could be necessary to re-configure the `log-source`

To get help from us send an email at support@nozominetworks.com, stating your problem and any detail that could help us solve the issue, please also attach /var/log/qradar.error. There might be also some information in your browser's console, please send that along too making sure all of the error is clearly visible and actionable.