

Aquí os dejamos una guía gráfica de los pasos para crear Dashboards Avanzados

# Community Request

Uno de nuestros clientes realizó una publicación en nuestra Community a la que queríamos darle solución.

The screenshot shows a post in a community forum. The post title is "1. Offense Close Reasons". It was posted by a user named DAVID SANZ POZAS, whose profile picture is a placeholder icon. The post was made 10 days ago and has 0 recommendations. The content of the post is:

I need to make a report or a widget to pulse that can visualize how the offenses were closed during the previous day, but I can't, in the default Qradar reports the reason for closing does not appear and in the Qradar API I also do not find how to extract the reason for each closed offense.  
any ideas?  
Regards

DAVID SANZ POZAS

<https://community.ibm.com/community/user/home>

# API Selection

IBM QRadar

Menu

- Dashboard**
- Offenses**
- Log Activity**
- Network Activity**
- Assets**
- Reports**
- Risks**
- Vulnerabilities**
- Use Case Manager**
- QWorkbench**
- Pulse**
- REST Test Development**

Network Activity (Event Count)

My Offenses

No results were returned for this item.

Most Severe Offenses

Offense Name	Magnitude
Massive file update detected - potential Malware containing Windows File System Folder or File Update	Red
Scan Followed By Successful Login preceded by Login Failures Followed By Success from the same Source IP preceded by Excessive Firewall Denies Between Hosts preceded by Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Firewall Drop	Yellow
Actual action: All actions failed preceded by Security risk found	Yellow
Flow Source/Interface Stopped Sending Flows	Yellow

Most Recent Offenses

Offense Name	Magnitude
Massive file update detected - potential Malware containing Windows File System Folder or File Update	Red
Flow Source/Interface Stopped Sending Flows	Yellow
Scan Followed By Successful Login preceded by Login Failures Followed By Success from the same Source IP preceded by Excessive Firewall Denies Between Hosts preceded by Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Firewall Drop	Yellow
Actual action: All actions failed preceded by Security risk found	Yellow

Top Services Denied through Firewalls (Event Count)

There was no Time Series data for the search performed.

[View in Log Activity](#)

IPS (Event Count)

Admin

QRadar Help Contents

About

Interactive API for Developers

# API Selection

## API Documentation

Home

API Version: 16.0

- access
- analytics
- ariel
- asset\_model
- auth
- backup\_and\_restore
- bandwidth\_manager
- config
- data\_classification**
- disaster\_recovery
- dynamic\_search
- forensics
- siem**
  - local\_destination\_addresses
  - offense\_closing\_reasons**
  - offense\_saved\_search\_delete\_
  - offense\_saved\_search\_depend
  - offense\_saved\_search\_groups
  - offense\_saved\_searches
  - offense\_types
  - offenses**
  - source\_addresses

### Interactive API Documentation for Developers

Welcome to the interactive API documentation for developers. Use the left navigation to access the documentation for the various API endpoints. This documentation provides information integrations with QRadar Security Intelligence Platform.

Use a non-production environment to test new API calls. Enter sample parameters and use the "Try it out!" button on each API endpoint page to make a real API request on your system.

To help you get started, see the following resources:

- The Reference section of the [Knowledge Center](#) for your QRadar release contains the RESTful API Guide. Navigate to the relevant version of QRadar, under the Reference section
- Use the [QRadar Support forum](#) to see questions and answers about using the API endpoints
- For information on ways to integrate with the API endpoints, see the [code samples on GitHub](#). The examples are written in Python, and include introductory samples and more complex examples.

# API Selection

API Documentation admin

Home

API Version: 16.0

- > access
- > analytics
- > ariel
- > asset\_model
- > auth
- > backup\_and\_restore
- > bandwidth\_manager
- > config
- > data\_classification
- > disaster\_recovery
- > dynamic\_search
- > forensics
- > gui\_app\_framework
- > health
- > health\_data
- > help
- > qni
- > qrm
- > qvm
- > reference\_data
- > reference\_data\_collections
- > scanner
- > services
- > siem
  - > local\_destination\_addresses
  - > offense\_closing\_reasons
  - > offense\_saved\_search\_delete
  - > offense\_saved\_search\_depend
  - > offense\_saved\_search\_groups
  - > offense\_saved\_searches
  - > offense\_types
  - > offenses**
  - > source\_addresses
- > staged\_config
- > system

**GET**

**16.0 - GET - /siem/offenses**

```
        "description": "String",
        "rules": [
            {
                "id": 42,
                "type": "String <one of: ADE_RULE, BUILDING_BLOCK_RULE, CRE_RULE>"
            }
        ],
        "event_count": 42,
        "flow_count": 42,
        "assigned_to": "String",
        "security_category_count": 42
    }
```

**Parameters**

Parameter	Type	Value	Data Type	MIME Type	Sample	Description
fields	Query	<input type="text" value="id,closing_reason_id"/>	String	text/plain	field_one (field_two, field_three),field_four	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	Query	<input type="text" value="status=CLOSED"/>	String	text/plain	field_one = "String" and field_two > 42 or not field_three in (1, 2, 3)	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
sort	Query	<input type="text" value=""/>	String	text/plain	+field_one,-object(sub_field)	Optional - This parameter is used to sort the elements in a list.
Range	Header	<input type="text" value=""/>	String	text/plain	items=0-5	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

**cURL**

```
curl -S -X GET -u admin -H 'Version: 16.0' -H 'Accept: application/json' 'https://172.16.60.60/api/siem/offenses?fields=id%20closing_reason_id&filter=status%3D%22CLOSED%22'
```

Activate Windows 10  
Go to Settings to activate Windows.

**Try It Out!**

# APP Editor

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Use Case Manager QWorkbench Pulse

Admin

Deploy Changes Advanced ▾

⚠ There are undeployed changes. Click Deploy Changes' to deploy them. View Details

Device Import

QRadar Log Source Management

QRadar Log Source Management

QRadar Use Case Manager

Configuration API Docs

Pulse - Dashboard

Pulse - Threat Globe

Threat Globe Configuration

QRadar App Editor

Develop Applications

The screenshot shows the IBM QRadar web interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin (which is highlighted with a red box), Use Case Manager, QWorkbench, and Pulse. On the left, a sidebar titled 'Admin' contains sections for System Configuration, Data Sources, Remote Networks and Services Configuration, and Apps. The main content area displays several management tools: 'Device Import', 'QRadar Log Source Management', 'QRadar Use Case Manager' (with links for Configuration and API Docs), 'Pulse - Dashboard', 'Pulse - Threat Globe' (with Threat Globe Configuration), and 'QRadar App Editor' (with a red box around it and a link for Develop Applications). A prominent yellow banner at the top indicates 'undeployed changes' with a 'Deploy Changes' button and a 'View Details' link.

# APP Editor

IBM QRadar App Editor

⚠️ QRadar App Editor only supports the upload of natively built UBI 8 applications. If you want to convert your Centos 6 application see the following documentation: [Migrating from App Framework V1 to V2](#)

## New App

Start from a simple starter app and begin development.

## Existing App

Upload or git clone an existing app and begin development.

## Resources

[Dev Centre](#) QRadar app development portal.

[Support Forum](#) Ask questions and find answers for common app development issues.

[Sample Apps](#) Github repository with QRadar sample apps.

[qpylib](#) Python library providing utility functions for QRadar apps.

[qjslib](#) Javascript library providing utility functions for QRadar apps.

## Videos

[Videos](#) IBM QRadar App Editor videos.

Activate  
Go to Settings

# APP Editor

Select a template

Hello World - Custom Tab

Enter a name for your Application

Hello World - Custom Tab

Give your Application a description

An example app to show Hello World in a custom tab

Set your Application's version

1.0.0

Set your Application's base image

qradar-app-base:2.0.5

[Cancel](#) [Install](#)

Select a template

Hello World - Custom Tab

API Version

As Root

Cache Control

Custom Columns Assets

Custom Columns Offenses

Custom Columns Offenses Globalized

Dashboard with Image

QPyLib Encryption

Environmental Variables

GUI Actions

Hello World

IP Metadata Provider

Memory Resource Configuration

Multiple UI Components

Multitenancy

Proxy

REST Method

⚠ QRadar App Editor only supports the upload of natively built UBI 8 applications. If you want to convert your Centos 6 application see the following documentation: [Migrating from App Framework V1 to V2](#)

Select a template

REST Method

Enter a name for your Application

REST Method test

Give your Application a description

test

Set your Application's version

1.0

Set your Application's base image

qradar-app-base:2.0.5

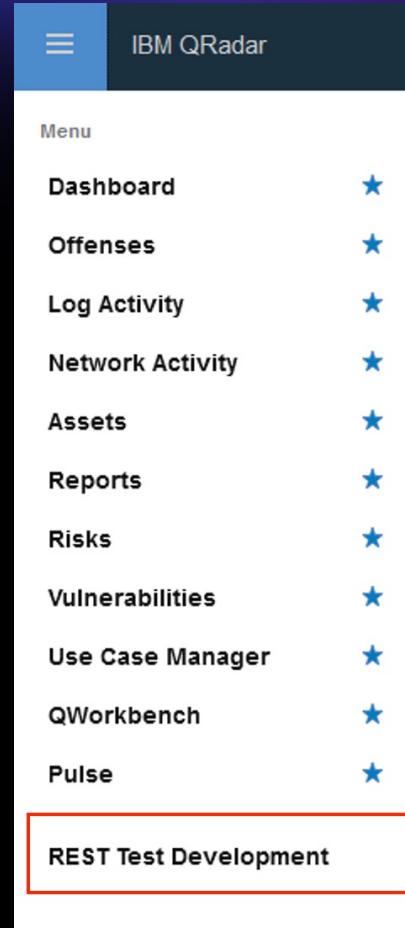
Cancel Install

## Existing App

Upload or git clone an existing app and begin development.

App install in progress | Stage 5 of 5: QRadar is installing the application [app\_id: 1167]... ⌚

# App Editor Deployment



The image shows a screenshot of the IBM QRadar mobile application's navigation menu. The menu is presented in a vertical list with each item followed by a blue star icon. A red rectangular box highlights the last item in the list, "REST Test Development".

- ☰ IBM QRadar
- Menu
- Dashboard ★
- Offenses ★
- Log Activity ★
- Network Activity ★
- Assets ★
- Reports ★
- Risks ★
- Vulnerabilities ★
- Use Case Manager ★
- QWorkbench ★
- Pulse ★
- REST Test Development

# App Editor Deployment

The screenshot shows the IBM QRadar App Editor interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Use Case Manager, QWorkbench, Pulse, and REST Test Development. Below this is a secondary navigation bar with IBM QRadar App Editor, File, Actions, and Help.

The main area features a file browser on the left and a code editor on the right. The file browser shows a directory structure:

- app-root
  - README.md
  - app
    - \_\_init\_\_.py
    - templates
      - views.py
  - manifest.json

The code editor displays the contents of the `views.py` file:

```
1  # Copyright 2020 IBM Corporation
2  #
3  # Licensed under the Apache License, Version 2.0 (the "License");
4  # you may not use this file except in compliance with the License.
5  # You may obtain a copy of the License at
6  #
7  #     http://www.apache.org/licenses/LICENSE-2.0
8  #
9  # Unless required by applicable law or agreed to in writing, software
10 # distributed under the License is distributed on an "AS IS" BASIS,
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
12 # See the License for the specific language governing permissions and
13 # limitations under the License.
14
15 from flask import Blueprint, render_template
16 import json
17 from qpylib import qpylib
18
19 # pylint: disable=invalid-name
20 viewsbp = Blueprint('views', __name__, url_prefix='/')
21
22
23 # An endpoint that populates a dropdown with Ariel database names using REST api call.
24 @viewsbp.route('/getArielDBList')
25 def get_ariel_databases():
26     try:
27         ariel_databases = qpylib.REST('get', '/api/ariel/databases')
28         options = {}
29         for db_name in ariel_databases.json():
30             options[db_name] = db_name
31             qpylib.log("Ariel DB name: " + db_name)
32         item = {
33             'id': 'ArielDBs',
34             'title': 'Ariel DB names',
35             'HTML': render_template('ariel.html', options=options)
36         }
37         return json.dumps(item)
38     except Exception as ex:
39         qpylib.log(
40             'Error calling REST api GET /api/ariel/databases: ' + str(ex),
41             'ERROR')
42         raise
```

# App Editor

IBM QRadar App Editor

File ▾ Actions ▾ Help ▾

Search...



app-root

- README.md
- app
  - \_\_init\_\_.py
  - templates
  - views.py
- manifest.json

views.py \* manifest.json

```
4 "# you may not use this file except in compliance with the license.
5 # You may obtain a copy of the License at
6 #
7 #     http://www.apache.org/licenses/LICENSE-2.0
8 #
9 # Unless required by applicable law or agreed to in writing, software
10 # distributed under the License is distributed on an "AS IS" BASIS,
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
12 # See the License for the specific language governing permissions and
13 # limitations under the License.
14
15 from flask import Blueprint, render_template
16 import json
17 from qpylib import qpylib
18
19 # pylint: disable=invalid-name
20 viewsbp = Blueprint('views', __name__, url_prefix='/')
21
22
23
24 @viewsbp.route('/getOffenses')
25 def getOffenses():
26     try:
27         api_1 = '/api/siem/offense_closing_reasons'
28         headers = {'content-type': 'application/json'}
29         response_closing = qpylib.REST('GET', api_1, headers=headers)
30         closing_reason = response_closing.json()
31         api_2 = '/api/siem/offenses?fields=id%2Cclosing_reason_id&filter=status%3D%22CLOSED%22'
32         response_offenses = qpylib.REST('GET', api_2, headers=headers)
33         offenses = response_offenses.json()
34         result = []
35         for reason in closing_reason:
36             calculo = {}
37             calculo['id']=reason['id']
38             calculo['text']=reason['text']
39             calculo['count'] = 0
40             for ofensa in offenses:
41                 if ofensa['closing_reason_id'] == reason['id']:
42                     calculo['count'] = calculo['count'] + 1
43             result.append(calculo)
44
45     except Exception as e:
46         qpylib.log(str(e), level='ERROR')
47     return json.dumps(result)
```

Search... ⟳ ☰

app-root

- README.md
- app
  - \_\_init\_\_.py
  - templates
  - ariel.html
- views.py

manifest.json

Deploy App..

Export App..

Delete App

In Development Mode

In Live Mode

Right 2020 IBM Corporation

```

3 # Licensed under the Apache License, Version 2.0 (the "License");
4 # you may not use this file except in compliance with the License.
5 # You may obtain a copy of the License at
6 #
7 #     http://www.apache.org/licenses/LICENSE-2.0
8 #
9 # Unless required by applicable law or agreed to in writing, software
10 # distributed under the License is distributed on an "AS IS" BASIS,
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
12 # See the License for the specific language governing permissions and
13 # limitations under the License.
14
15 from flask import Blueprint, render_template
16 import json
17 from qpylib import qpylib
18
19 # pylint: disable=invalid-name
20 viewsbp = Blueprint('views', __name__, url_prefix='/')
21
22
23 # An endpoint that populates a dropdown with Ariel database names using REST api call.
24 @viewsbp.route('/getOffenses')
25 def getOffenses():
26     try:
27         api_1 = '/api/siem/offense_closing_reasons'
28         headers = {'content-type' : 'application/json'}
29         response_closing = qpylib.REST('GET', api_1, headers=headers)
30         closing_reason = response_closing.json()
31         api_2 = '/api/siem/offenses?fields=id%2C%20closing_reason_id&filter=status%3D%22CLOSED%22'
32         response_offenses = qpylib.REST('GET', api_2, headers=headers)
33         offenses = response_offenses.json()
34         result = []
35         for reason in closing_reason:
36             calculo = {}
37             calculo['id']=reason['id']
38             calculo['text']=reason['text']
39             calculo['count'] = 0
40             for ofensa in offenses:
41                 if ofensa['closing_reason_id'] == reason['id']:
42                     calculo['count'] = calculo['count'] + 1
43             result.append(calculo)
44
45     except Exception as e:
46         qpylib.log(str(e), level='ERROR')
47
48     return json.dumps(result)

```

**Download Application Zip**

Before deploying it is highly recommended you download a copy of your application zip. Would you like to do so now?

No

Yes

**Confirm Application Deploy**

During application deployment, the editor will be unavailable. This should only take a few minutes and then you will be prompted to refresh QRadar. Are you sure you want to continue?

No

Yes

**Application is Upgrading...**

This dialog will update once complete

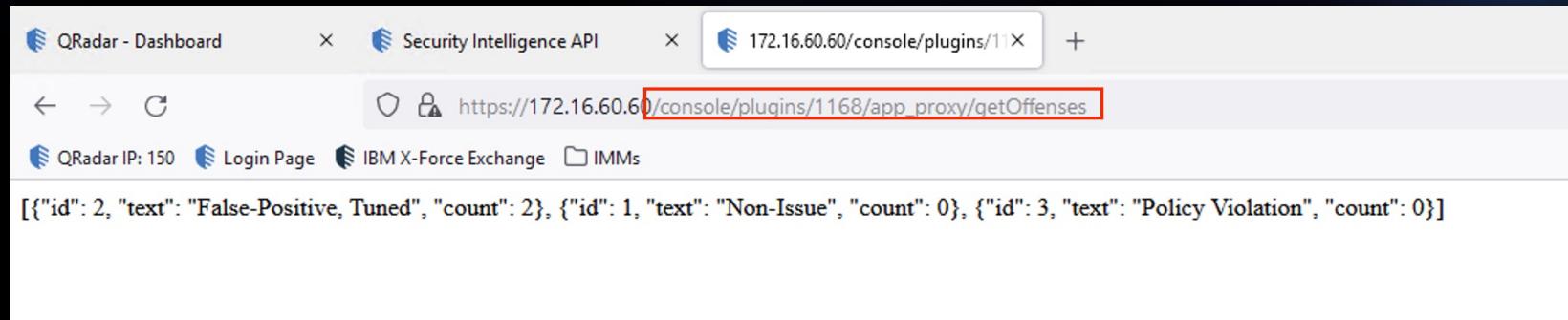
**Application Upgrade Successful**

Application upgrade has completed successfully. Please refresh QRadar to see your changes.

Please refresh your browser to continue.

Refresh

# App Editor Deployment



A screenshot of a web browser window. The title bar shows three tabs: "QRadar - Dashboard", "Security Intelligence API", and "172.16.60.60/console/plugins/11X". The active tab is the third one. Below the tabs is a navigation bar with back, forward, and refresh buttons. The address bar displays the URL "https://172.16.60.60/console/plugins/1168/app\_proxy/getOffenses". A red box highlights this URL. Below the address bar is a menu bar with links: "QRadar IP: 150", "Login Page", "IBM X-Force Exchange", and "IMMs". The main content area of the browser shows a JSON array of offense data:

```
[{"id": 2, "text": "False-Positive, Tuned", "count": 2}, {"id": 1, "text": "Non-Issue", "count": 0}, {"id": 3, "text": "Policy Violation", "count": 0}]
```

# Custom Pulse Dashboard

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Use Case Manager QWorkbench Pulse System Time: 5:15 PM

Dashboard Offense overview

**My Offenses**  
A few seconds ago

Magnitude	Description
1	Large Outbound Transfer Slow Rate of Transfer preceded by Large Ou...

**Number of Offenses**  
A few seconds ago

4

**Critical Offenses**  
A few seconds ago

0

**High Offenses**  
A few seconds ago

0

**Top offense categories**  
A few seconds ago

Category	Count
Successful File Modification	2
System Failure,Misc,Web,Unk...	4
Web,Data Loss Possible	2
Warning	1
User Login Failure,Misc Log...	5
Firewall Deny,ACL Deny,User...	7

Magnitude Description

1d 1d

3 Massive file update detected - potential Malware containing Wi...

1 Flow Source/Interface Stopped Sending Flows

1 Large Outbound Transfer Slow Rate of Transfer preceded by Lar...

# Custom Pulse Dashboard

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Use Case Manager QWorkbench Pulse System Time: 5:15 PM

Configure dashboard

## Offense overview

Use these default dashboards as a starting point to create your own customized dashboards.

Q What are you looking for today?

Create new widget

Create and configure a new widget that will be saved to your library.

+ 

Time series chart  Active offenses over time

Active offenses

Created by admin Modified on 11/8/2021

Tabular display  Most recent offenses

Most recent offenses

Created by admin Modified on 11/8/2021

Tabular display  Most severe offenses

Most severe offenses

Created by admin Modified on 11/8/2021

Tabular display  My Offenses

My Offenses

Created by admin Modified on 11/8/2021

Big number chart  Number of critical offenses

Critical Offenses

Created by admin Modified on 11/8/2021

Big number chart  Number of high offenses

High Offenses

Created by admin Modified on 11/8/2021

Big number chart  Open Offenses

Number of Offenses

Created by admin Modified on 11/8/2021

8 widgets selected Deselect all <https://172.16.60.60>

Cancel Save Go to Settings to activate Windows.

# Custom Pulse Dashboard

^ Query

Data source \* Refresh Time

Generic API Every Minute

URL endpoint

/console/plugins/1168/app\_proxy/getOffenses

Results mapping

JSON path to the results (e.g. data.items).

Use title from the result set

Off

**Run Query**

Results

ID	Text	Count
2	False-Positive, Tuned	2
1	Non-Issue	0
3	Policy Violation	0

\* Showing 3 of 3 results from 11/15/2021.

# Custom Pulse Dashboard

New dashboard item

View Name \*

 ...

Chart Type \*

 ▼

General Format Drilldown

Label \*

 ▼

Value \*

 ▼

Doughnut Chart

Off

Show Legend

Yes

Legend Orientation

Vertical ▼

Preview

A pie chart titled "Preview" showing the distribution of offense closing reasons. The chart is divided into three segments: a large blue segment representing "Policy Violation" at 50%, a medium orange segment representing "False-Positive, Tuned" at 33.3%, and a smaller green segment representing "Non-issue" at 16.7%. The segments are labeled with their respective percentages.

Reason	Percentage
Policy Violation	50%
False-Positive, Tuned	33.3%
Non-issue	16.7%

Cancel Save Activate Windows  
Go to Settings to activate Windows.

# Custom Pulse Dashboard

IBM QRadar

System Time: 5:23 PM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Use Case Manager QWorkbench Pulse

Offense overview

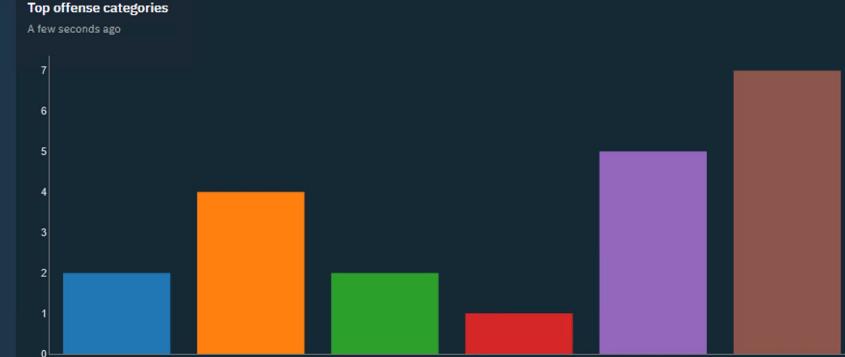
Most recent offenses

A few seconds ago

Magnitude	Description	Id
3	Massive file update detected - potential Malware containing Wi...	6
1	Flow Source/Interface Stopped Sending Flows	5
1	Large Outbound Transfer Slow Rate of Transfer preceded by Lar...	4

Top offense categories

A few seconds ago



Category	Magnitude
Successful File Modification	2
System Failure,Misc,Web,Unk...	4
Web,Data Loss Possible	2
Warning	1
User Login Failure,Misc Log...	5
Firewall Deny,ACL Deny,User...	7

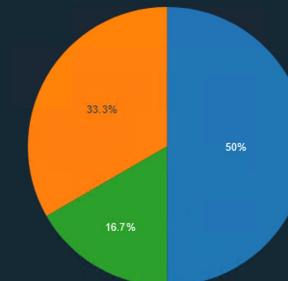
Most severe offenses

A few seconds ago

Magnitude	Description
3	Massive file update detected - potential Malware containing Windows...
2	Scan Followed By Successful Login preceded by Login Failures Follow...
2	Actual action: All actions failed preceded by Security risk found
1	Flow Source/Interface Stopped Sending Flows

Offenses Closing Reason

A few seconds ago



Reason	Percentage
Policy Violation	50%
False-Positive, Tuned	33.3%
Non-Issue	16.7%

Activate Windows  
Go to Settings to activate Windows.