In order to work with antivirus and logs, we will add a new agent.

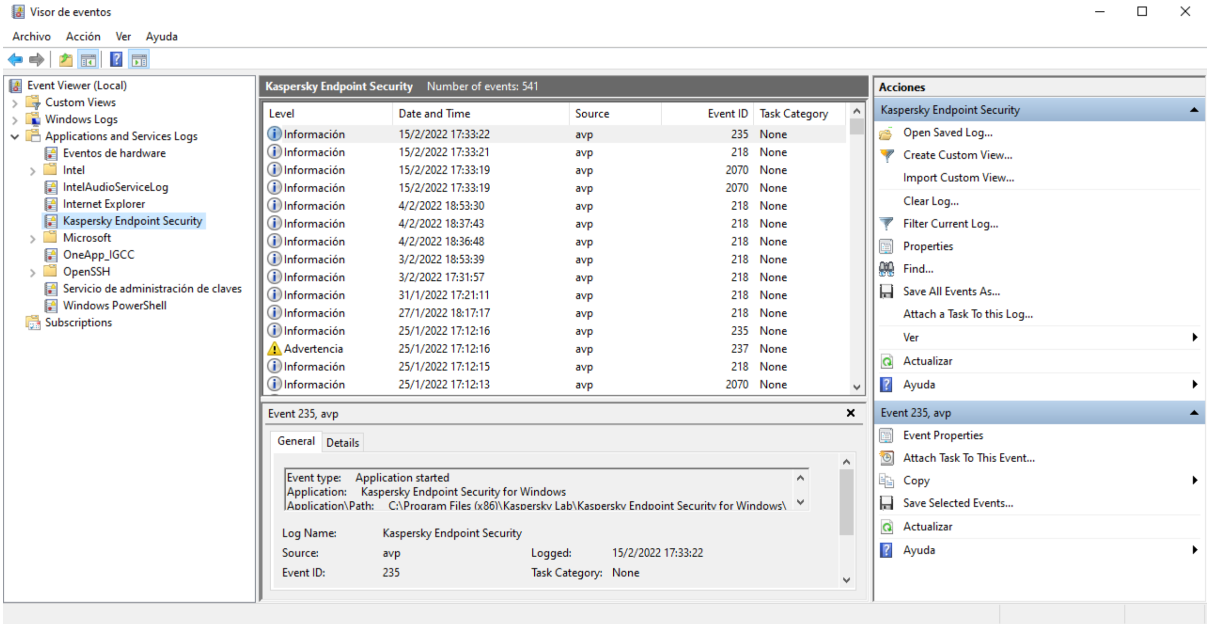
Agent 3.

```
OS: Microsoft Windows 10 Pro 10.0.19042
IP: 192.168.128.89
Name: B70017351361129
```

The chosen antivirus is Kaspersky, is the one that we found that best matches with the functionalities that Wazuh provide us.

First we have to identify where are the Kaspersky logs and events.

Unlike other antivirus, we can find his monitoring in *Windows Events Viewer > Applications and Services Logs > Kaspersky Endpoint Security*. This will be the reference of our channel in Wazuh.



Kaspersky Endpoint Security Number of events: 541

Level	Date and Time	Source	Event ID	Task Category
Información	15/2/2022 17:33:22	avp	235	None
Información	15/2/2022 17:33:21	avp	218	None
Información	15/2/2022 17:33:19	avp	2070	None
Información	15/2/2022 17:33:19	avp	2070	None
Información	4/2/2022 18:53:30	avp	218	None
Información	4/2/2022 18:37:43	avp	218	None
Información	4/2/2022 18:36:48	avp	218	None
Información	3/2/2022 18:53:39	avp	218	None
Información	3/2/2022 17:31:57	avp	218	None
Información	31/1/2022 17:21:11	avp	218	None
Información	27/1/2022 18:17:17	avp	218	None
Información	25/1/2022 17:12:16	avp	235	None
Advertencia	25/1/2022 17:12:16	avp	237	None
Información	25/1/2022 17:12:15	avp	218	None
Información	25/1/2022 17:12:13	avp	2070	None

Event 235, avp

General Details

```
Event type:    Application started
Application:    Kaspersky Endpoint Security for Windows
Application\Path:    C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\
```

Log Name: Kaspersky Endpoint Security
Source: avp   Logged: 15/2/2022 17:33:22
Event ID: 235   Task Category: None

Figure 1: "Events viewer"

The next point is add this reference in our agent *ossec.conf*. We can also add this information in the wazuh manager if we have this agent in a group.

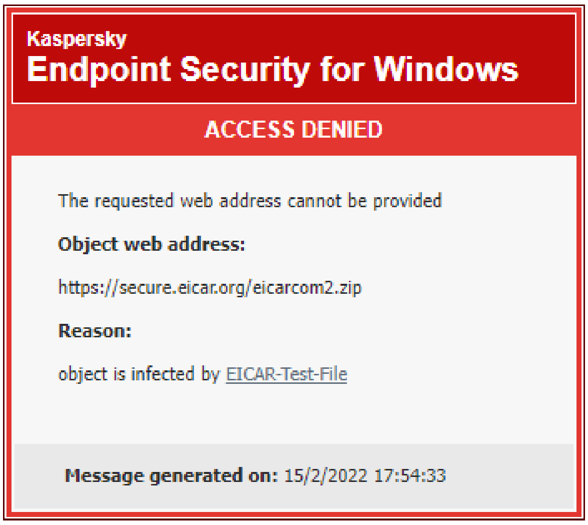
```
  <localfile>
    <location>Kaspersky Endpoint Security</location>
    <log_format>eventchannel</log_format>
  </localfile>
```

Now we save and restart the Wazuh agent service.

To check if it works, we will force Kaspersky alerts that will add events that we will capture and we will be able to monitour in our Wazuh manager. We can do it accessing to these files in our navigator:

- https://secure.eicar.org/eicar.com)
- https://secure.eicar.org/eicar.com.txt
- https://secure.eicar.org/eicar_com.zip

- https://secure.eicar.org/eicarcom2.zip



Kaspersky
Endpoint Security for Windows

ACCESS DENIED

The requested web address cannot be provided

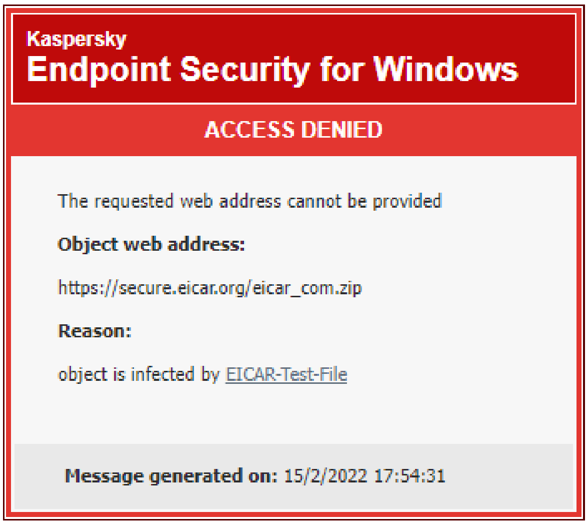
Object web address:

https://secure.eicar.org/eicarcom2.zip

Reason:

object is infected by EICAR-Test-File

Message generated on: 15/2/2022 17:54:33



Kaspersky
Endpoint Security for Windows

ACCESS DENIED

The requested web address cannot be provided

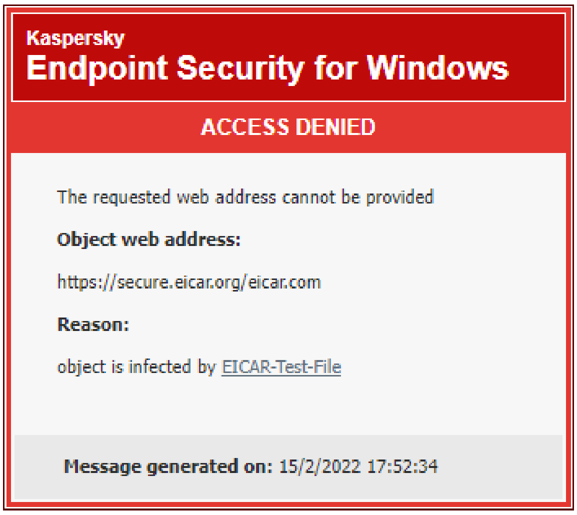
Object web address:

https://secure.eicar.org/eicar_com.zip

Reason:

object is infected by EICAR-Test-File

Message generated on: 15/2/2022 17:54:31



Kaspersky
Endpoint Security for Windows

ACCESS DENIED

The requested web address cannot be provided

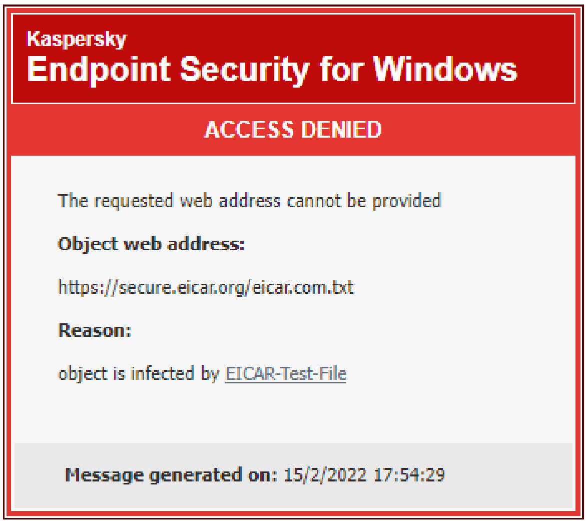
Object web address:

https://secure.eicar.org/eicar.com

Reason:

object is infected by EICAR-Test-File

Message generated on: 15/2/2022 17:52:34



Kaspersky
Endpoint Security for Windows

ACCESS DENIED

The requested web address cannot be provided

Object web address:

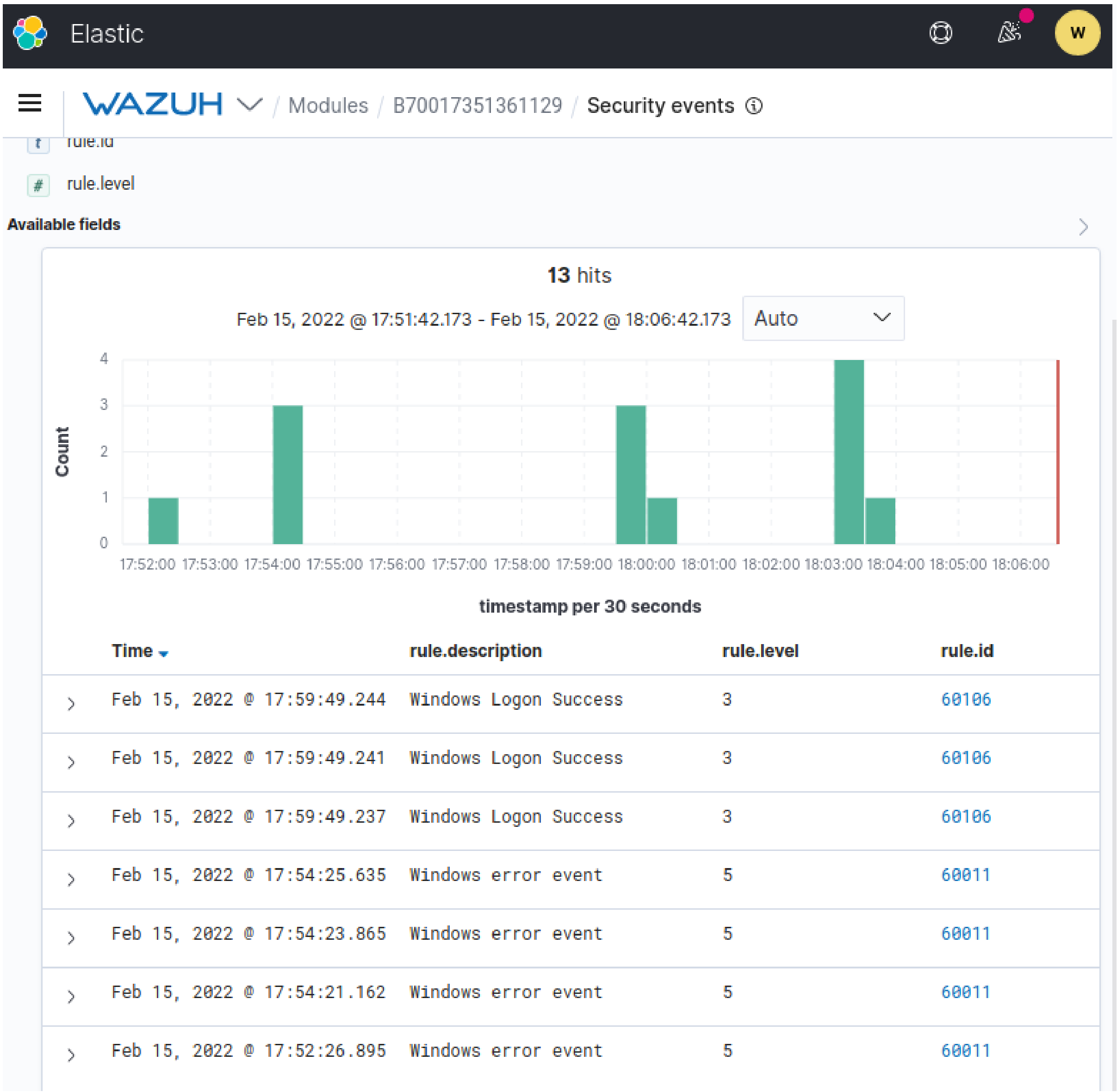
https://secure.eicar.org/eicar.com.txt

Reason:

object is infected by EICAR-Test-File

Message generated on: 15/2/2022 17:54:29

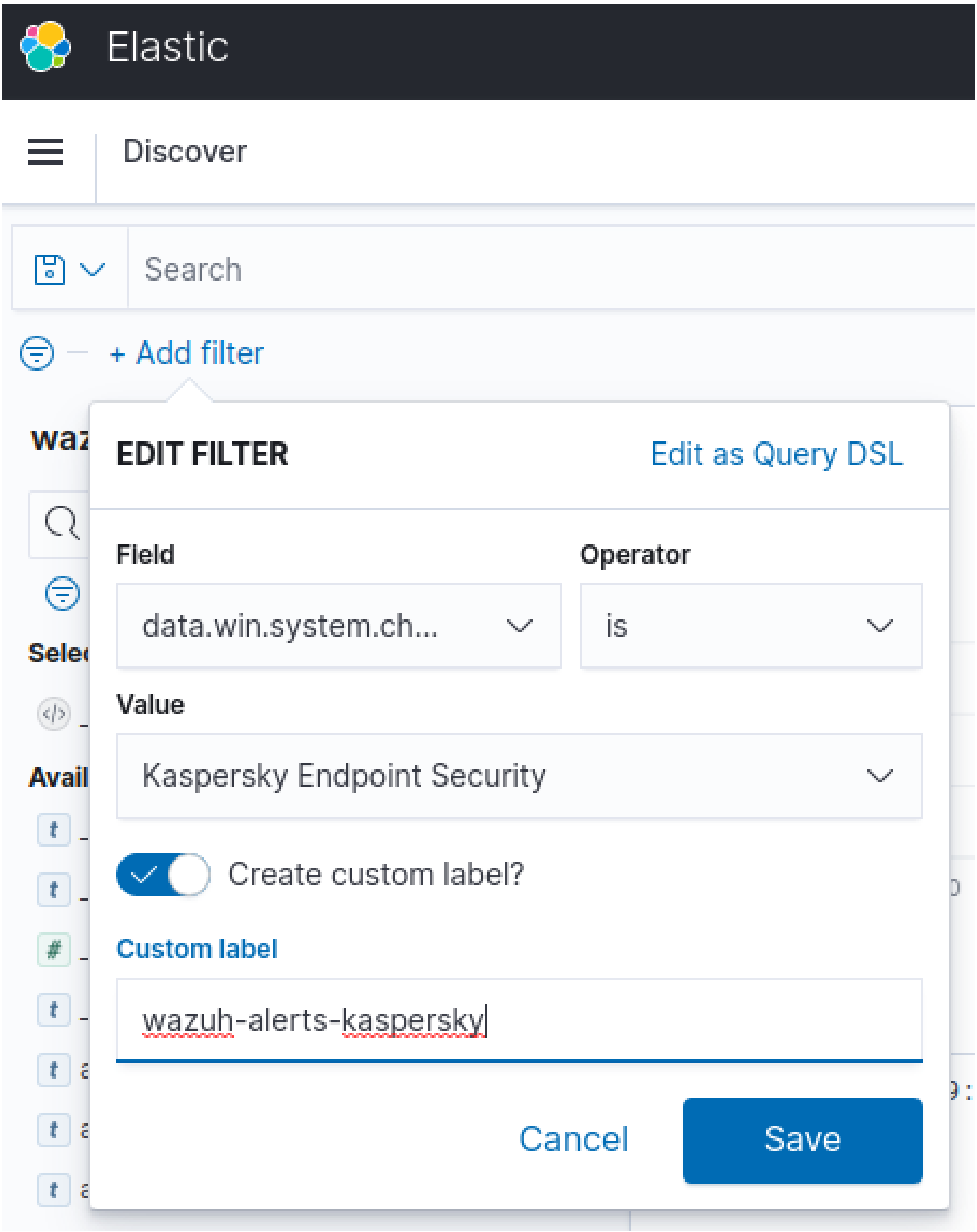
If we go to the *Security events* screen of our agent we can monitor these events and see the events that we force.



Time	rule.description	rule.level	rule.id
Feb 15, 2022 @ 17:59:49.244	Windows Logon Success	3	60106
Feb 15, 2022 @ 17:59:49.241	Windows Logon Success	3	60106
Feb 15, 2022 @ 17:59:49.237	Windows Logon Success	3	60106
Feb 15, 2022 @ 17:54:25.635	Windows error event	5	60011
Feb 15, 2022 @ 17:54:23.865	Windows error event	5	60011
Feb 15, 2022 @ 17:54:21.162	Windows error event	5	60011
Feb 15, 2022 @ 17:52:26.895	Windows error event	5	60011

Figure 2: “Security events”

To see only the Kaspersky events we can add a custom filter.



Field: data.win.system.ch...

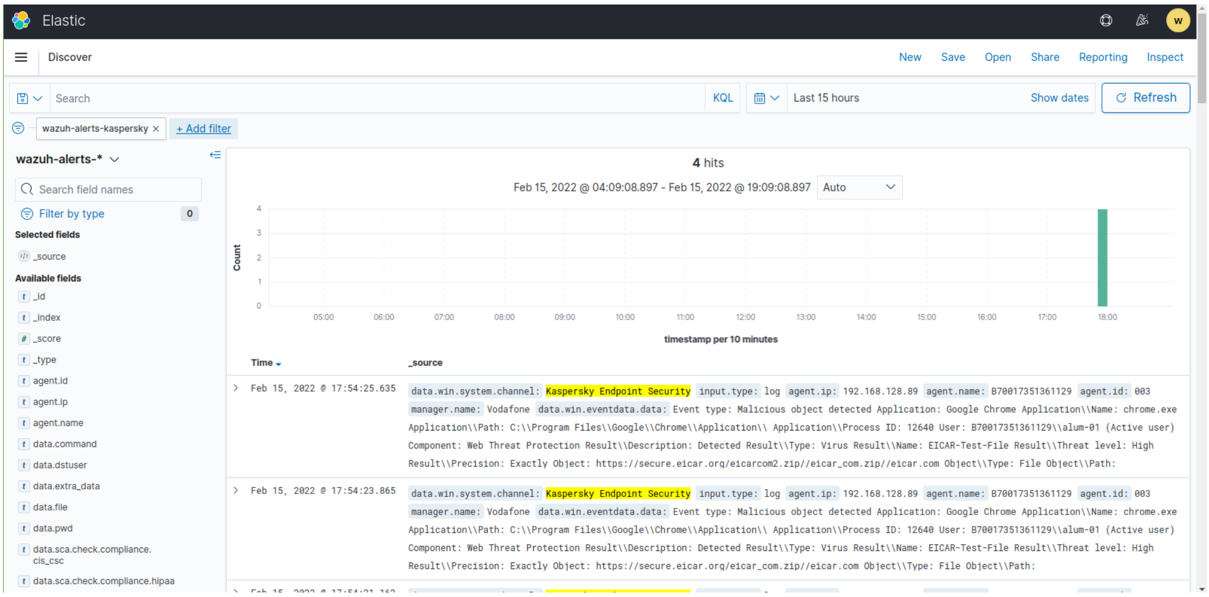
Operator: is

Value: Kaspersky Endpoint Security

Create custom label? ✓

Custom label: wazuh-alerts-kaspersky

Figure 3: "Add filter"



```
Feb 15, 2022 @ 17:54:25.635   data.win.system.channel: Kaspersky Endpoint Security input.type: log agent.ip: 192.168.128.89 agent.name: B70017351361129 agent.id: 003
                              manager.name: Vodafone data.win.eventdata.data: Event type: Malicious object detected Application: Google Chrome Application\\Name: chrome.exe
                              Application\\Path: C:\\Program Files\\Google\\Chrome\\Application\\ Application\\Process ID: 12640 User: B70017351361129\\alum-01 (Active user)
                              Component: Web Threat Protection Result\\Description: Detected Result\\Type: Virus Result\\Name: EICAR-Test-File Result\\Threat level: High
                              Result\\Precision: Exactly Object: https://secure.eicar.org/eicarcom2.zip//eicar_com.zip//eicar.com Object\\Type: File Object\\Path:

Feb 15, 2022 @ 17:54:23.865   data.win.system.channel: Kaspersky Endpoint Security input.type: log agent.ip: 192.168.128.89 agent.name: B70017351361129 agent.id: 003
                              manager.name: Vodafone data.win.eventdata.data: Event type: Malicious object detected Application: Google Chrome Application\\Name: chrome.exe
                              Application\\Path: C:\\Program Files\\Google\\Chrome\\Application\\ Application\\Process ID: 12640 User: B70017351361129\\alum-01 (Active user)
                              Component: Web Threat Protection Result\\Description: Detected Result\\Type: Virus Result\\Name: EICAR-Test-File Result\\Threat level: High
                              Result\\Precision: Exactly Object: https://secure.eicar.org/eicar_com.zip//eicar.com Object\\Type: File Object\\Path:
```

Figure 4: “Filtered logs”

The events can be exported in JSON format.

Attached the exported information:

```
{
  "_index": "wazuh-alerts-4.x-2022.02.15",
  "_type": "_doc",
  "_id": "rZxO_n4BMzeLMS_HizTP",
  "_version": 1,
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "192.168.128.89",
      "name": "B70017351361129",
      "id": "003"
    },
    "manager": {
      "name": "Vodafone"
    },
    "data": {
      "win": {
        "eventdata": {
          "data": "Event type:     Malicious object detected
             Application:     Google Chrome Application\\\\Name:
             chrome.exe Application\\\\Path:     C:\\\\Program Files
             \\\\Google\\\\Chrome\\\\Application\\\\ Application\\\\
             Process ID:     12640 User:     B70017351361129\\\\alum
             -01 (Active user) Component:     Web Threat Protection
             Result\\\\Description:     Detected Result\\\\Type:
             Virus Result\\\\Name:     EICAR-Test-File Result\\\\
             Threat level:     High Result\\\\Precision:     Exactly
             Object:     https://secure.eicar.org/eicarcom2.zip//
             eicar_com.zip//eicar.com Object\\\\Type:     File Object
```

```
           \\\\Path:     https://secure.eicar.org/eicarcom2.zip//
           eicar_com.zip//eicar.com Object\\\\Name:     eicar.com
           Reason:     Expert analysis Database release date:
           24/9/2021 13:20:00 Hash:     275
           a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
           "
      },
      "system": {
        "eventID": "302",
        "keywords": "0x80000000000000",
        "level": "2",
        "channel": "Kaspersky Endpoint Security",
        "opcode": "0",
        "message": "\"Event type:     Malicious object detected\
           nApplication:     Google Chrome\nApplication\\Name:
           chrome.exe\nApplication\\Path:     C:\\Program Files\\
           Google\\Chrome\\Application\\\nApplication\\Process ID:
               12640\nUser:     B70017351361129\\alum-01 (Active
           user)\nComponent:     Web Threat Protection\nResult\\
           Description:     Detected\nResult\\Type:     Virus\
           nResult\\Name:     EICAR-Test-File\nResult\\Threat level:
                High\nResult\\Precision:     Exactly\nObject:
           https://secure.eicar.org/eicarcom2.zip//eicar_com.zip//
           eicar.com\nObject\\Type:     File\nObject\\Path:
           https://secure.eicar.org/eicarcom2.zip//eicar_com.zip//
           eicar.com\nObject\\Name:     eicar.com\nReason:
           Expert analysis\nDatabase release date:     24/9/2021
           13:20:00\nHash:     275
           a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
           \n\"",
        "version": "0",
        "systemTime": "2022-02-15T16:54:33.6036745Z",
        "eventRecordID": "545",
        "threadID": "0",
        "computer": "B70017351361129",
        "task": "0",
        "processID": "0",
        "severityValue": "ERROR",
        "providerName": "avp"
      }
    }
  },
  "rule": {
    "firedtimes": 4,
    "mail": false,
    "level": 5,
    "description": "Windows error event",
    "groups": [
      "windows",
      "system_error"
    ],
    "id": "60011",
    "gpg13": [
      "4.3"
    ],
    "gdpr": [
      "IV_35.7.d"
    ]
    },
    "location": "EventChannel",
    "decoder": {
      "name": "windows_eventchannel"
    },
    "id": "1644944065.1549830",
    "timestamp": "2022-02-15T17:54:25.635+0100"
  },
  "fields": {
    "timestamp": [
      "2022-02-15T16:54:25.635Z"
    ]
  },
  "highlight": {
    "agent.id": [
      "@kibana-highlighted-field@003@/kibana-highlighted-field@"
    ],
    "manager.name": [
      "@kibana-highlighted-field@Vodafone@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1644944065635
  ]
}
```

```
{
  "_index": "wazuh-alerts-4.x-2022.02.15",
  "_type": "_doc",
  "_id": "rJxO_n4BMzeLMS_HhzTn",
  "_version": 1,
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "192.168.128.89",
      "name": "B70017351361129",
      "id": "003"
    },
    "manager": {
      "name": "Vodafone"
    },
    "data": {
      "win": {
        "eventdata": {
          "data": "Event type:     Malicious object detected
              Application:     Google Chrome Application\\\\Name:
              chrome.exe Application\\\\Path:     C:\\\\Program Files
              \\\\Google\\\\Chrome\\\\Application\\\\ Application\\\\
              Process ID:     12640 User:     B70017351361129\\\\alum
              -01 (Active user) Component:     Web Threat Protection
              Result\\\\Description:     Detected Result\\\\Type:
              Virus Result\\\\Name:     EICAR-Test-File Result\\\\
              Threat level:     High Result\\\\Precision:     Exactly
              Object:     https://secure.eicar.org/eicar_com.zip//eicar
              .com Object\\\\Type:     File Object\\\\Path:     https
```

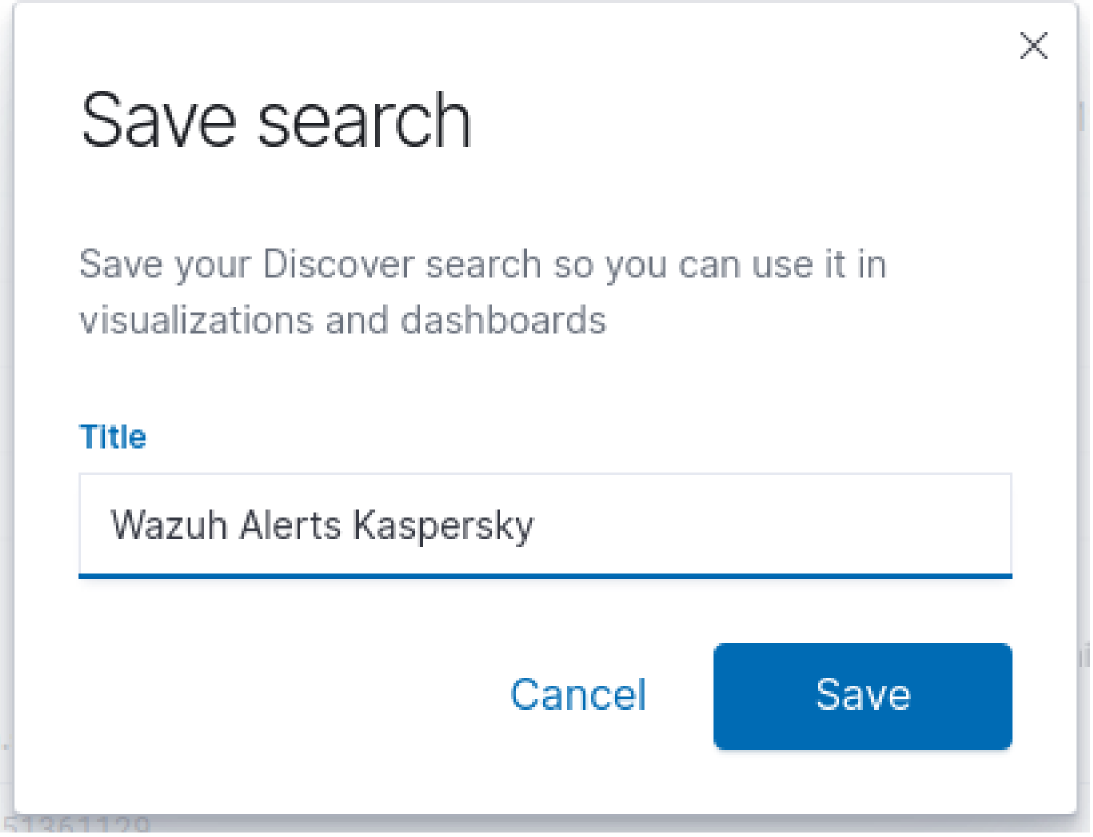
```
             ://secure.eicar.org/eicar_com.zip//eicar.com Object\\\
             Name:     eicar.com Reason:     Expert analysis Database
             release date:     24/9/2021 13:20:00 Hash:     275
             a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
             "
        },
        "system": {
          "eventID": "302",
          "keywords": "0x80000000000000",
          "level": "2",
          "channel": "Kaspersky Endpoint Security",
          "opcode": "0",
          "message": "\"Event type:     Malicious object detected\
             nApplication:     Google Chrome\nApplication\\Name:
             chrome.exe\nApplication\\Path:     C:\\Program Files\\
             Google\\Chrome\\Application\\\nApplication\\Process ID:
                 12640\nUser:     B70017351361129\\alum-01 (Active
             user)\nComponent:     Web Threat Protection\nResult\\
             Description:     Detected\nResult\\Type:     Virus\
             nResult\\Name:     EICAR-Test-File\nResult\\Threat level:
                  High\nResult\\Precision:     Exactly\nObject:
             https://secure.eicar.org/eicar_com.zip//eicar.com\nObject
             \\Type:     File\nObject\\Path:     https://secure.eicar.
             org/eicar_com.zip//eicar.com\nObject\\Name:     eicar.com
             \nReason:     Expert analysis\nDatabase release date:
                 24/9/2021 13:20:00\nHash:     275
             a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
             \n\"",
          "version": "0",
          "systemTime": "2022-02-15T16:54:31.8356917Z",
          "eventRecordID": "544",
          "threadID": "0",
          "computer": "B70017351361129",
          "task": "0",
          "processID": "0",
          "severityValue": "ERROR",
          "providerName": "avp"
        }
      }
    },
    "rule": {
      "firedtimes": 3,
      "mail": false,
      "level": 5,
      "description": "Windows error event",
      "groups": [
        "windows",
        "system_error"
      ],
      "id": "60011",
      "gpg13": [
        "4.3"
      ],
      "gdpr": [
        "IV_35.7.d"
      ]
    },
    "location": "EventChannel",
    "decoder": {
      "name": "windows_eventchannel"
    },
    "id": "1644944063.1545645",
    "timestamp": "2022-02-15T17:54:23.865+0100"
  },
  "fields": {
    "timestamp": [
      "2022-02-15T16:54:23.865Z"
    ]
  },
  "highlight": {
    "agent.id": [
      "@kibana-highlighted-field@003@/kibana-highlighted-field@"
    ],
    "manager.name": [
      "@kibana-highlighted-field@Vodafone@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1644944063865
  ]
}
```

```
{
  "_index": "wazuh-alerts-4.x-2022.02.15",
  "_type": "_doc",
  "_id": "q5xO_n4BMzeLMS_HfDRN",
  "_version": 1,
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "192.168.128.89",
      "name": "B70017351361129",
      "id": "003"
    },
    "manager": {
      "name": "Vodafone"
    },
    "data": {
      "win": {
        "eventdata": {
          "data": "Event type:     Malicious object detected
              Application:     Google Chrome Application\\\\Name:
              chrome.exe Application\\\\Path:     C:\\\\Program Files
              \\\\Google\\\\Chrome\\\\Application\\\\ Application\\\\
              Process ID:     12640 User:     B70017351361129\\\\alum
              -01 (Active user) Component:     Web Threat Protection
              Result\\\\Description:     Detected Result\\\\Type:
              Virus Result\\\\Name:     EICAR-Test-File Result\\\\
              Threat level:     High Result\\\\Precision:     Exactly
              Object:     https://secure.eicar.org/eicar.com.txt Object
              \\\\Type:     File Object\\\\Path:     https://secure.
              eicar.org/eicar.com.txt Object\\\\Name:     eicar.com.txt
               Reason:     Expert analysis Database release date:
                 24/9/2021 13:20:00 Hash:     275
                 a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
                 "
          },
          "system": {
            "eventID": "302",
            "keywords": "0x80000000000000",
            "level": "2",
            "channel": "Kaspersky Endpoint Security",
            "opcode": "0",
            "message": "\"Event type:     Malicious object detected\
                 nApplication:     Google Chrome\nApplication\\Name:
                 chrome.exe\nApplication\\Path:     C:\\Program Files\\
                 Google\\Chrome\\Application\\\nApplication\\Process ID:
                     12640\nUser:     B70017351361129\\alum-01 (Active
                 user)\nComponent:     Web Threat Protection\nResult\\
                 Description:     Detected\nResult\\Type:     Virus\
                 nResult\\Name:     EICAR-Test-File\nResult\\Threat level:
                      High\nResult\\Precision:     Exactly\nObject:
                 https://secure.eicar.org/eicar.com.txt\nObject\\Type:
                     File\nObject\\Path:     https://secure.eicar.org/
                 eicar.com.txt\nObject\\Name:     eicar.com.txt\nReason:
                     Expert analysis\nDatabase release date:     24/9/2021
                  13:20:00\nHash:     275
                 a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
                 \n\"",
            "version": "0",
            "systemTime": "2022-02-15T16:54:29.0471847Z",
            "eventRecordID": "543",
            "threadID": "0",
            "computer": "B70017351361129",
            "task": "0",
            "processID": "0",
            "severityValue": "ERROR",
            "providerName": "avp"
          }
        }
      },
      "rule": {
        "firedtimes": 2,
        "mail": false,
        "level": 5,
        "description": "Windows error event",
        "groups": [
          "windows",
          "system_error"
        ],
        "id": "60011",
        "gpg13": [
          "4.3"
        ],
        "gdpr": [
          "IV_35.7.d"
        ]
      },
      "location": "EventChannel",
      "decoder": {
        "name": "windows_eventchannel"
```

```
    },
    "id": "1644944061.1541532",
    "timestamp": "2022-02-15T17:54:21.162+0100"
  },
  "fields": {
    "timestamp": [
      "2022-02-15T16:54:21.162Z"
    ]
  },
  "highlight": {
    "agent.id": [
      "@kibana-highlighted-field@003@/kibana-highlighted-field@"
    ],
    "manager.name": [
      "@kibana-highlighted-field@Vodafone@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1644944061162
  ]
}
```

```
{
  "_index": "wazuh-alerts-4.x-2022.02.15",
  "_type": "_doc",
  "_id": "ppxM_n4BMzeLMS_HuzQY",
  "_version": 1,
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "192.168.128.89",
      "name": "B70017351361129",
      "id": "003"
    },
    "manager": {
      "name": "Vodafone"
    },
    "data": {
      "win": {
        "eventdata": {
          "data": "Event type:     Malicious object detected
              Application:     Google Chrome Application\\\\Name:
              chrome.exe Application\\\\Path:     C:\\\\Program Files
              \\\\Google\\\\Chrome\\\\Application\\\\ Application\\\\
              Process ID:     12640 User:     B70017351361129\\\\alum
              -01 (Active user) Component:     Web Threat Protection
              Result\\\\Description:     Detected Result\\\\Type:
              Virus Result\\\\Name:     EICAR-Test-File Result\\\\
              Threat level:     High Result\\\\Precision:     Exactly
              Object:     https://secure.eicar.org/eicar.com Object\\\\
              Type:     File Object\\\\Path:     https://secure.eicar.
              org/eicar.com Object\\\\Name:     eicar.com Reason:
              Expert analysis Database release date:     24/9/2021
              13:20:00 Hash:     275
              a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
              "
        },
        "system": {
          "eventID": "302",
          "keywords": "0x80000000000000",
          "level": "2",
          "channel": "Kaspersky Endpoint Security",
          "opcode": "0",
          "message": "\"Event type:     Malicious object detected\nApplication:     Google Chrome\nApplication\\Name:     chrome.exe\nApplication\\Path:     C:\\Program Files\\Google\\Chrome\\Application\\\nApplication\\Process ID:     12640\nUser:     B70017351361129\\alum-01 (Active user)\nComponent:     Web Threat Protection\nResult\\Description:     Detected\nResult\\Type:     Virus\nResult\\Name:     EICAR-Test-File\nResult\\Threat level:     High\nResult\\Precision:     Exactly\nObject:     https://secure.eicar.org/eicar.com\nObject\\Type:     File\nObject\\Path:     https://secure.eicar.org/eicar.com\nObject\\Name:     eicar.com\nReason:     Expert analysis\nDatabase release date:     24/9/2021 13:20:00\nHash:     275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f\n\"",
          "version": "0",
          "systemTime": "2022-02-15T16:52:34.8645210Z",
          "eventRecordID": "542",
          "threadID": "0",
          "computer": "B70017351361129",
          "task": "0",
          "processID": "0",
          "severityValue": "ERROR",
          "providerName": "avp"
        }
      }
    },
    "rule": {
      "firedtimes": 1,
      "mail": false,
      "level": 5,
      "description": "Windows error event",
      "groups": [
        "windows",
        "system_error"
      ],
      "id": "60011",
      "gpg13": [
        "4.3"
      ],
      "gdpr": [
        "IV_35.7.d"
      ]
    },
    "location": "EventChannel",
    "decoder": {
      "name": "windows_eventchannel"
    },
    "id": "1644943946.1537467",
    "timestamp": "2022-02-15T17:52:26.895+0100"
  },
  "fields": {
    "timestamp": [
      "2022-02-15T16:52:26.895Z"
    ]
  },
  "highlight": {
    "agent.id": [
      "@kibana-highlighted-field@003@/kibana-highlighted-field@"
    ],
    "manager.name": [
      "@kibana-highlighted-field@Vodafone@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1644943946895
  ]
}
```

We can save this search configuration to find it quickly, since it is information that we may want to monitor often.



Save search

Save your Discover search so you can use it in visualizations and dashboards

Title: Wazuh Alerts Kaspersky

Figure 5: “Save search”

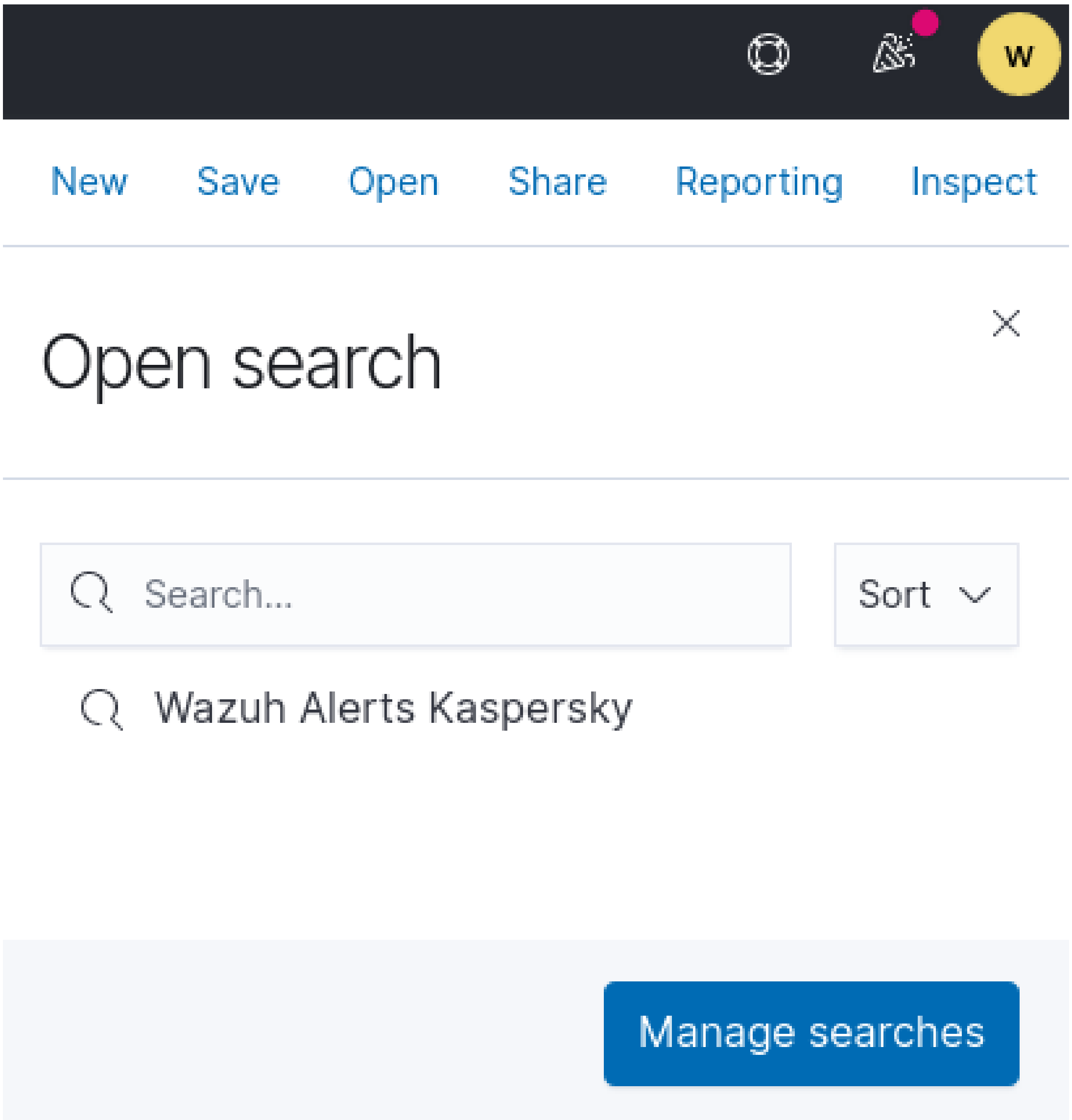


Figure 6: "Open search"

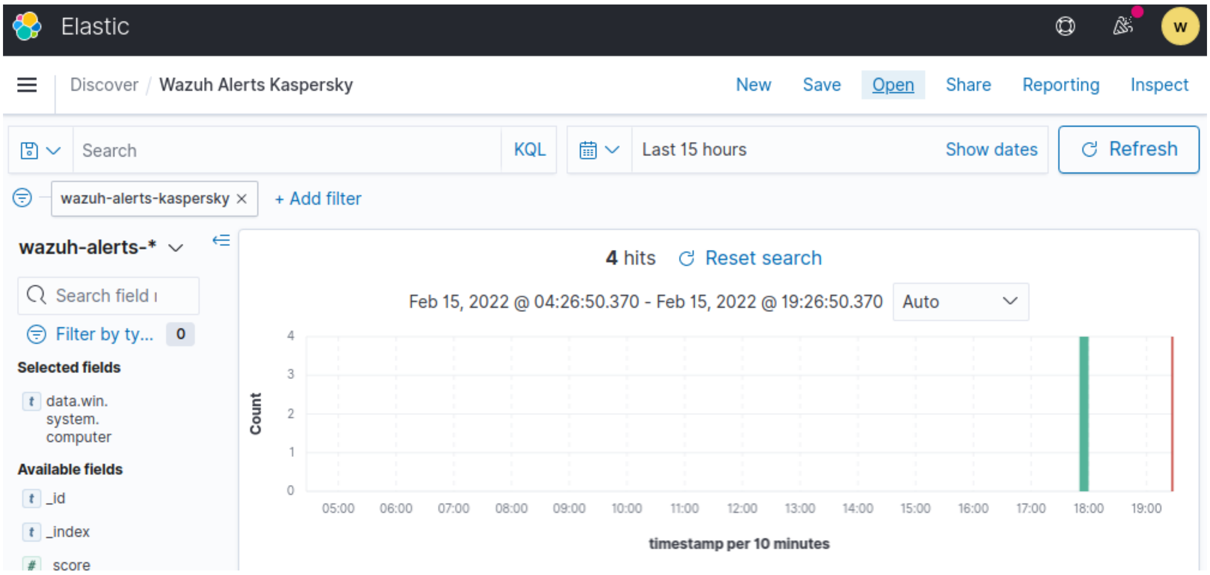
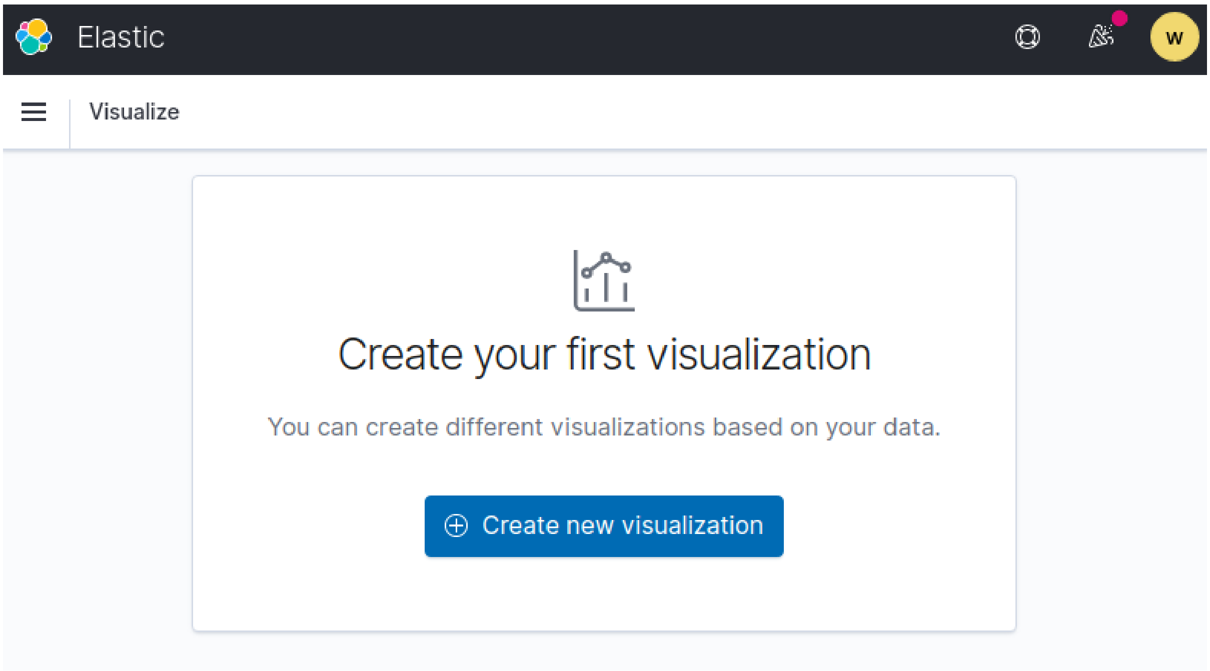


Figure 7: “Custom ‘Wazuh Alerts Kaspersky’ search”

We can also create custom dashboards to monitor what we want. A dashboard is organized with panels in a row and column structure. Thus, we can have different information with different time ranges in custom graphs.

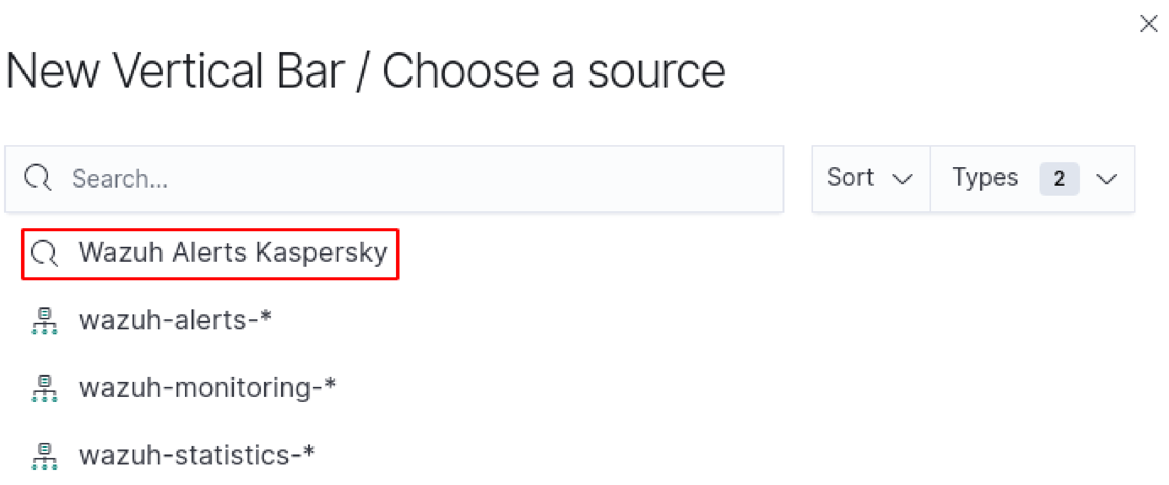
First of all, we will create a visualization bar chart with the number of kaspersky alerts per agent.



Create your first visualization

You can create different visualizations based on your data.

Figure 8: “Create visualitzation”



New Vertical Bar / Choose a source

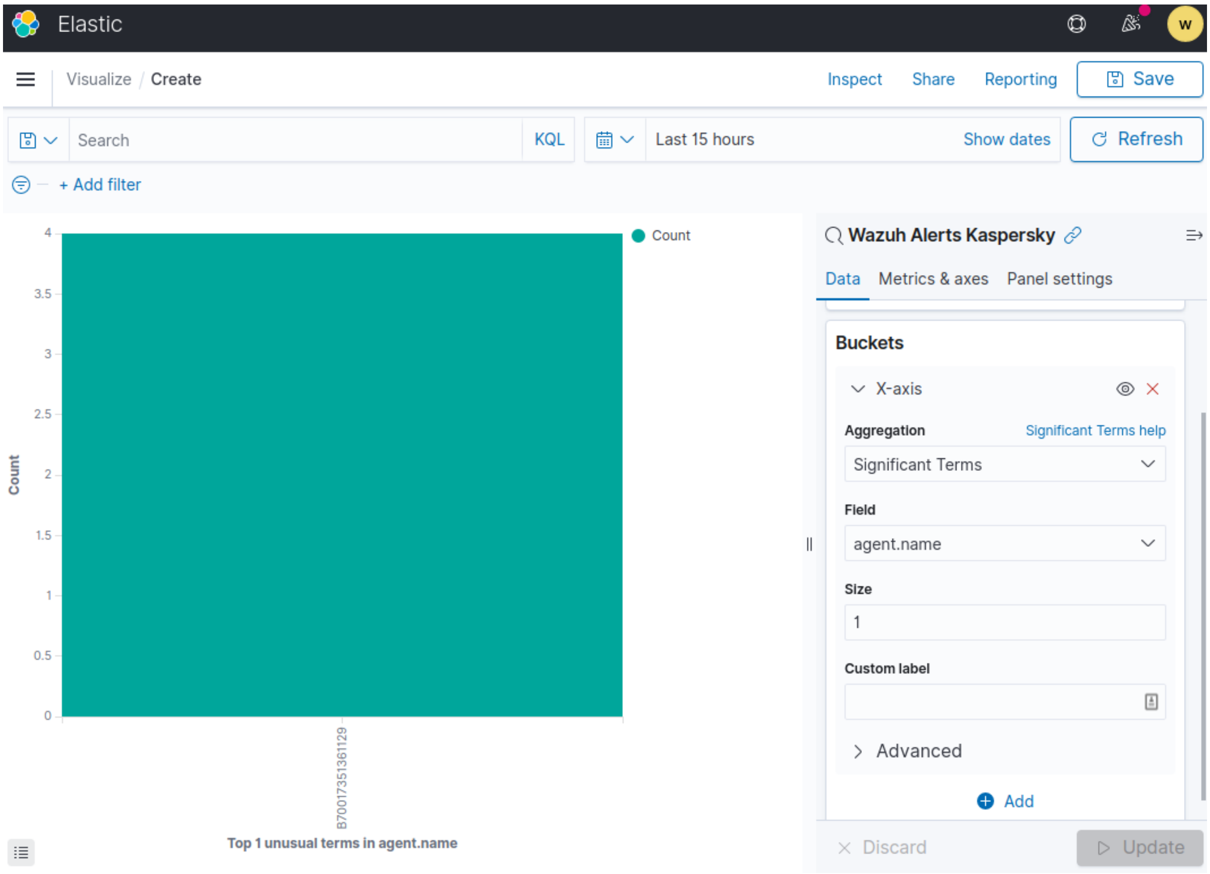
Wazuh Alerts Kaspersky

wazuh-alerts-*

wazuh-monitoring-*

wazuh-statistics-*

Figure 9: "Add graph"



Wazuh Alerts Kaspersky

Buckets

X-axis

Aggregation: Significant Terms

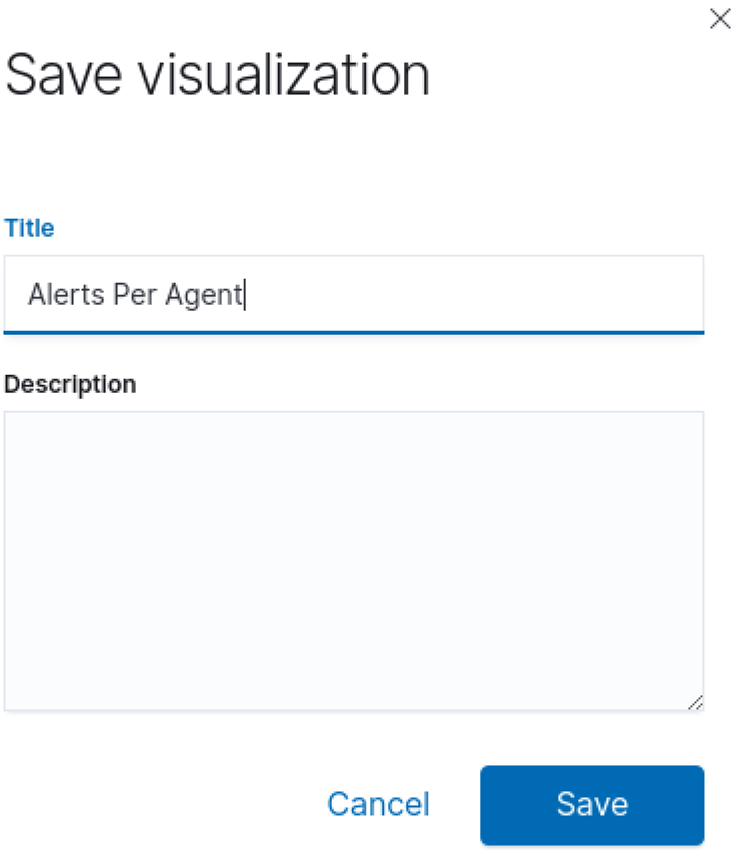
Field: agent.name

Size: 1

Custom label:

Advanced

Figure 10: "Create graph"



Save visualization

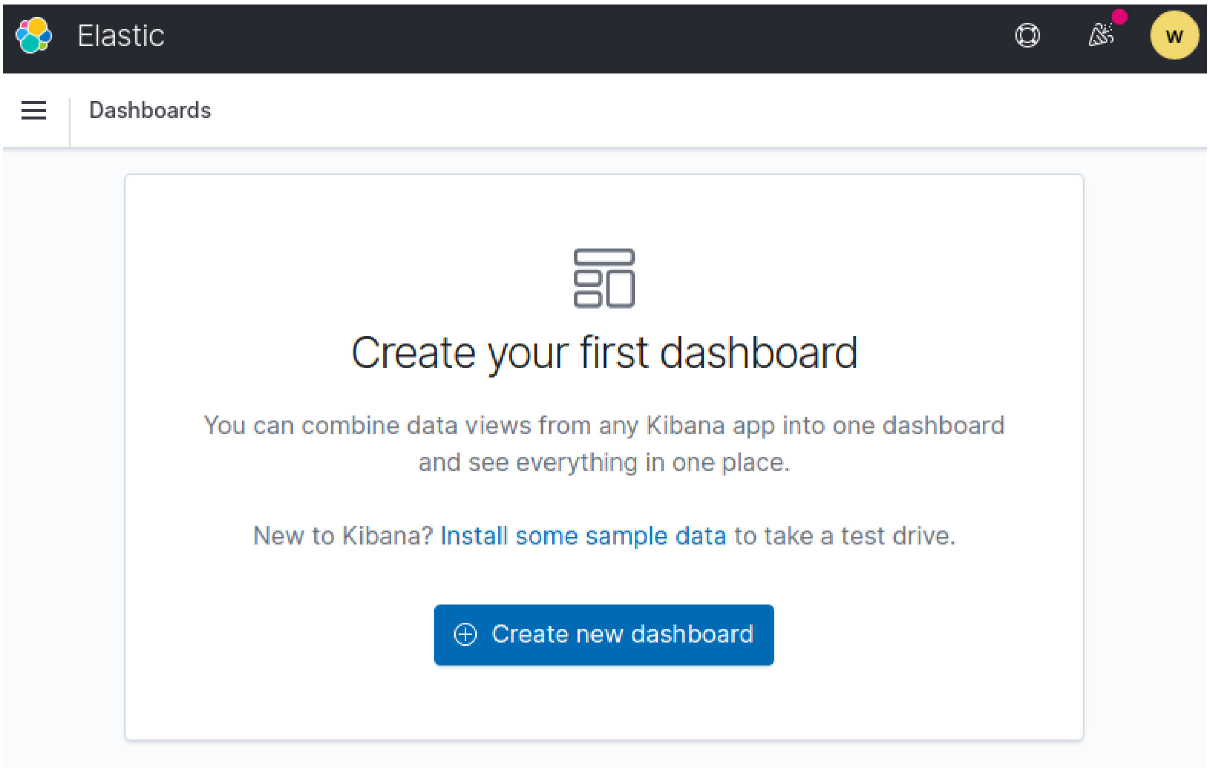
Title

Alerts Per Agent

Description

Figure 11: "Save visualization"

With the first element created, we proceed to create the dashboard.



Elastic

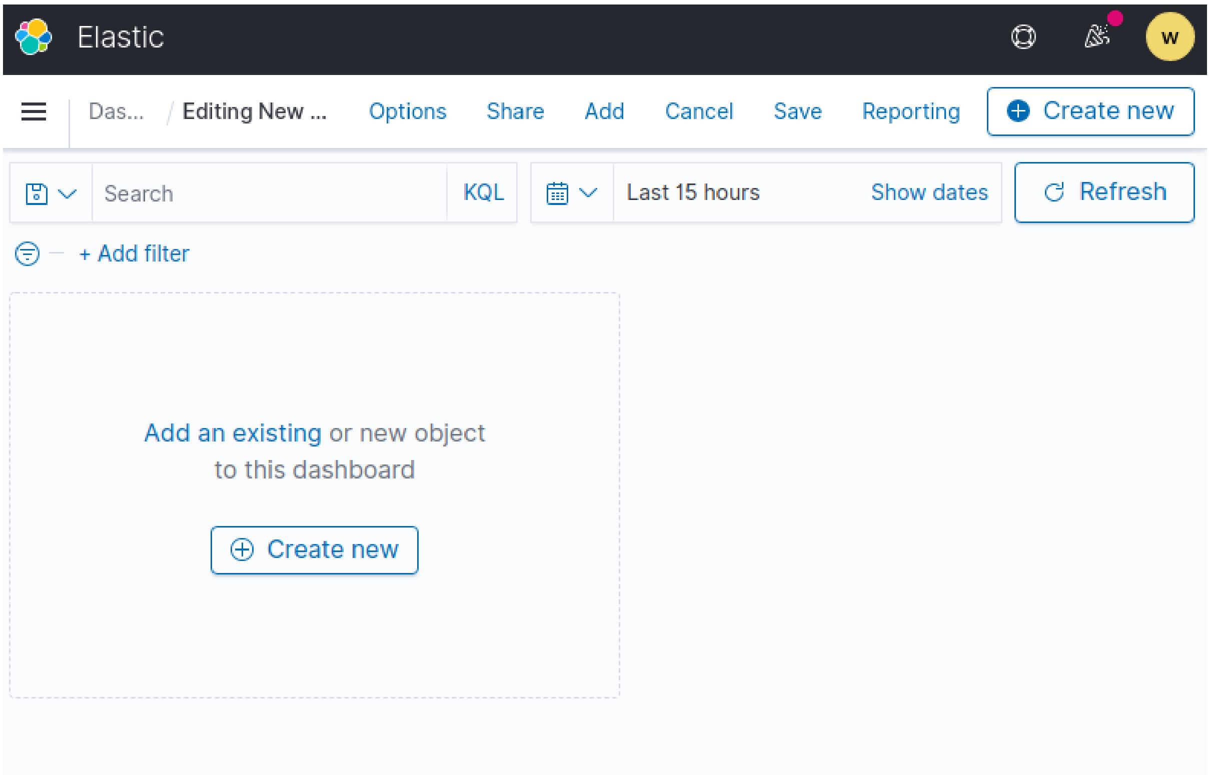
Dashboards

Create your first dashboard

You can combine data views from any Kibana app into one dashboard and see everything in one place.

New to Kibana? Install some sample data to take a test drive.

Figure 12: "Create dashboard"



Elastic

Add an existing or new object to this dashboard

Figure 13: "Editing dashboard"

We have created other panels to create a useful dashboard. Now we add each graph in a position

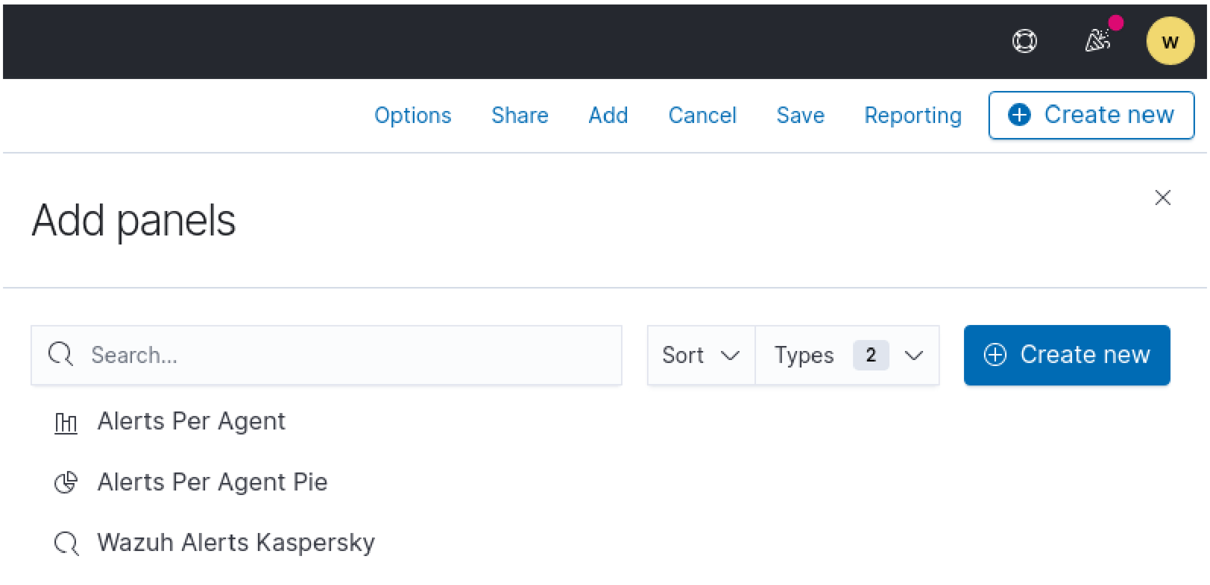


Figure 14: “Add panels to dashboard”

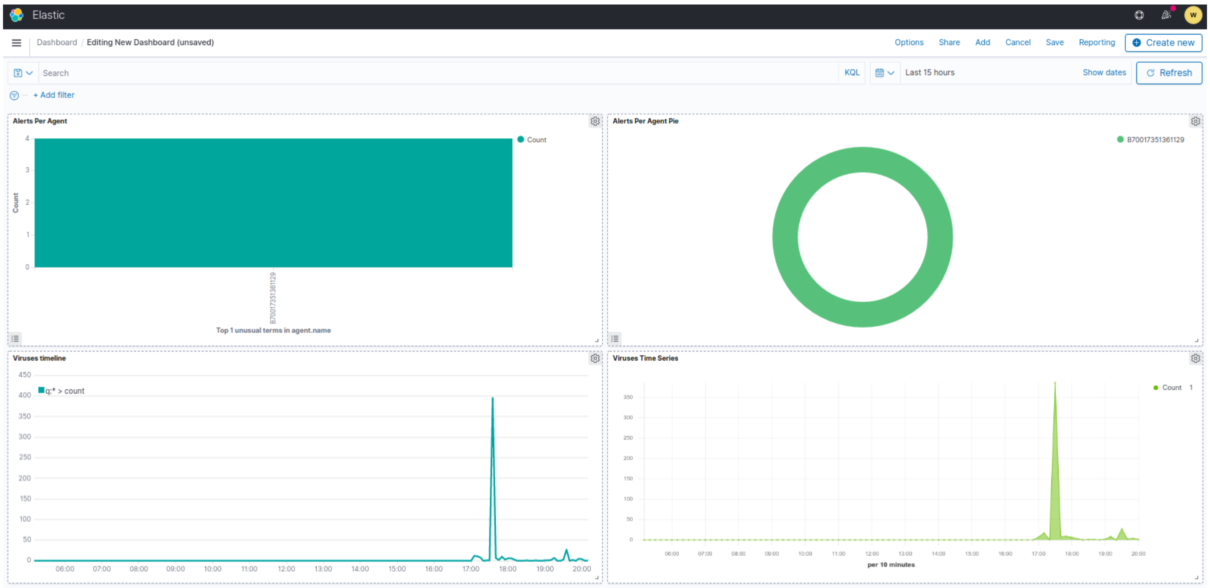
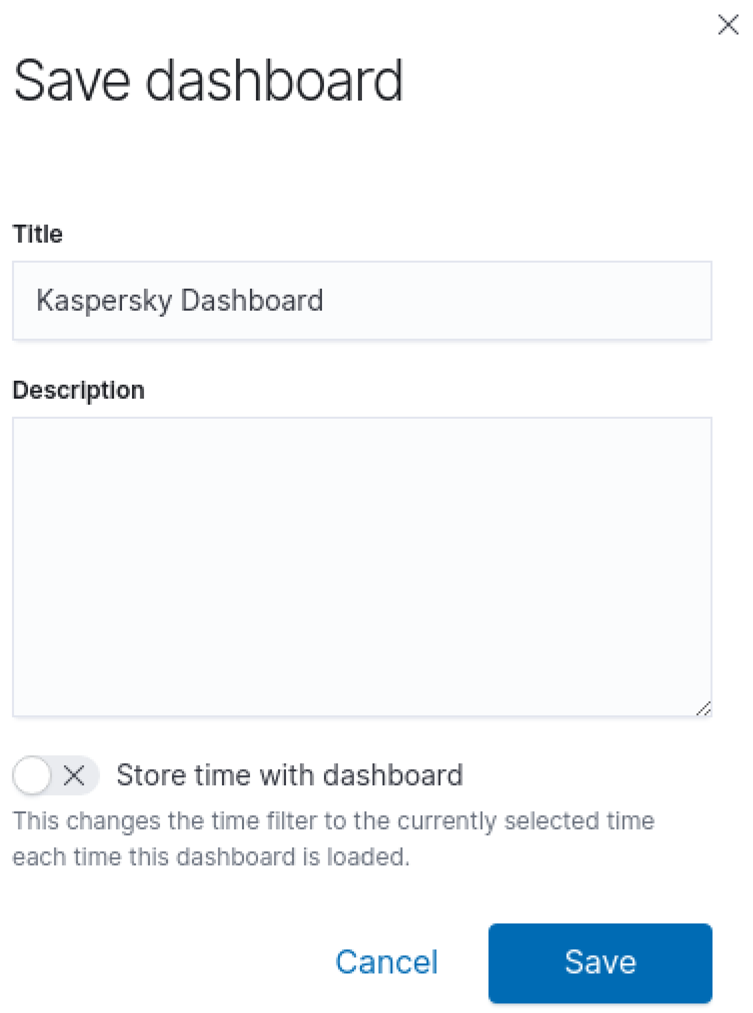


Figure 15: “Editing our dashboard”



Save dashboard

Title

Kaspersky Dashboard

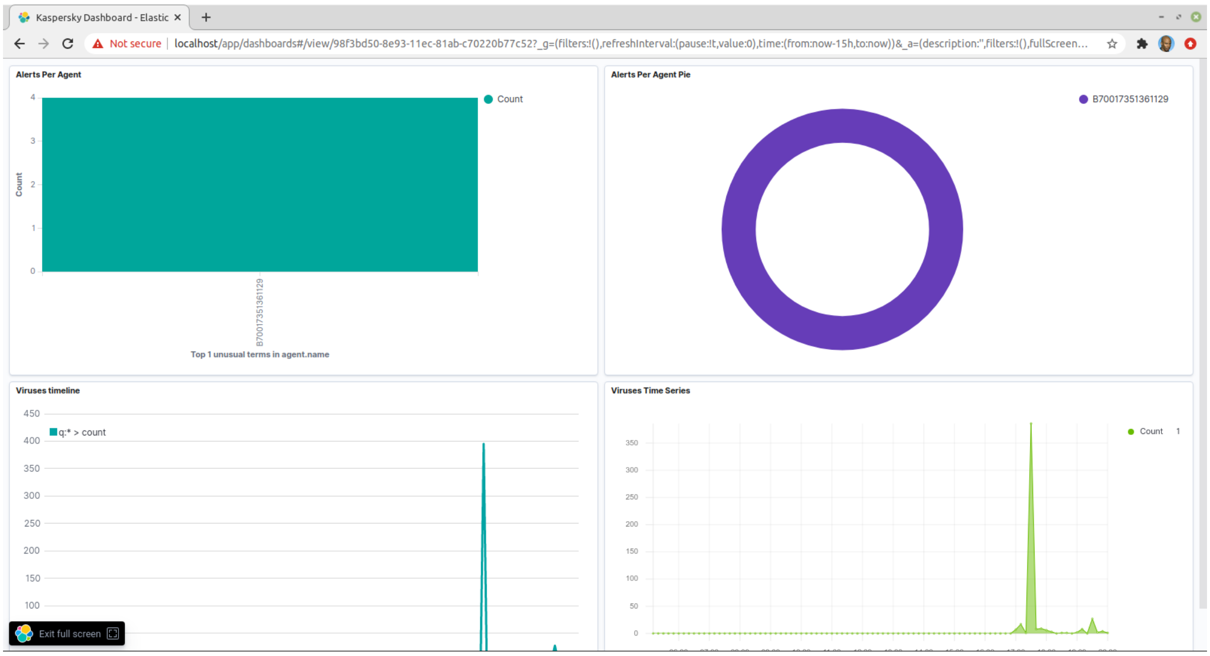
Description

Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Figure 16: “Save dashboard”

Now we can monitor the chosen information simply by opening our dashboard.



Kaspersky Dashboard - Elastic
Not secure
localhost/app/dashboards#/view/98f3bd50-8e93-11ec-81ab-c70220b77c52?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15h,to:now))&_a=(description:'',filters:!(),fullScreen...
Alerts Per Agent
4
3
2
1
0
Count
Count
B70017351361129
Top 1 unusual terms in agent.name
Alerts Per Agent Pie
B70017351361129
Viruses timeline
450
400
350
300
250
200
150
100
q:* > count
Exit full screen
Viruses Time Series
350
300
250
200
150
100
50
0
Count 1

Figure 17: “Kaspersky Dashboard”