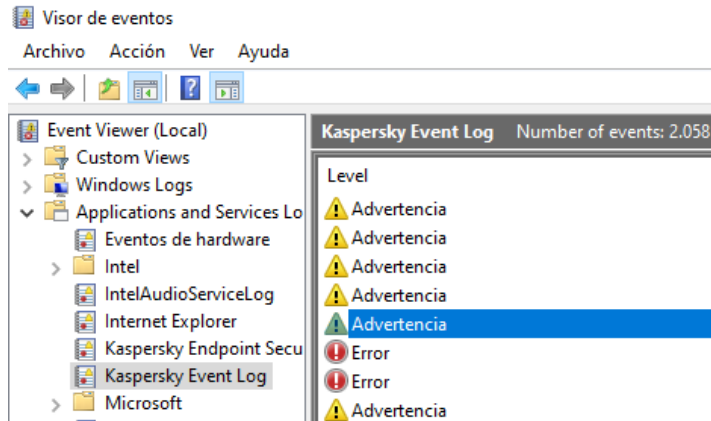


Podem configurar el Wazuh per rebre els logs generats pels antivirus de les màquines clients. Anem a veure-ho pel Kaspersky però el procediment és el mateix per a qualsevol altre:

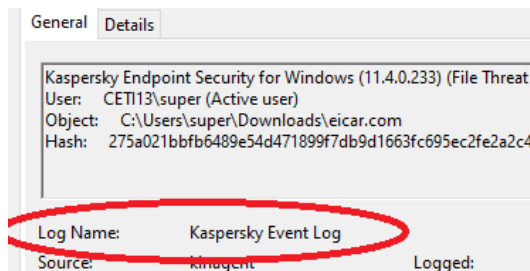
## Kaspersky

A la màquina client executa el visor d'events, selecciona *Applications and Services Logs* i selecciona *Kaspersky Event Log*.



Aquí pots veure totes les alertes que genera l'antivirus. El que farem ara és dir-li a l'agent Wazuh que agafi aquesta informació i l'envii al Wazuh manager.

En aquesta mateixa finestra dels logs de Kaspersky, en el detall de qualsevol log, hi ha el valor *Log Name*. D'aquí agafarem el valor per crear una directriu al fitxer *ossec.conf* de l'agent Wazuh.



A l'apartat `<!-- Log analysis -->` afegim-hi aquesta nova directriu:

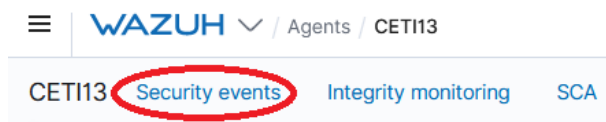
```
<localfile>
  <location>Kaspersky Event Log</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Desa els canvis i reinicia el servei.

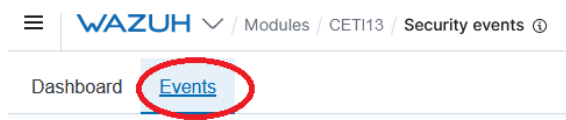
Per actualitzar l'agent des del Wazuh manager en comptes d'anar al client, posa aquesta directriu al grup al qual pertany la màquina.

Per comprovar una alerta, farem servir un *Antimalware Test File* que és un fitxer que simula un virus i s'utilitza per testear els antivirus. S'anomena *eicar.com* i el pots descarregar de la web [https://www.eicar.org/?page\\_id=3950](https://www.eicar.org/?page_id=3950)

Després d'executar el fitxer *eicar.com* i que l'antivirus el posi en quarentena, connecta't al Wazuh manager, ves a *Security events* de la màquina client:



Després selecciona Events:



I hauràs rebut una notificació:

Time	rule.description
> Feb 3, 2022 @ 18:18:38.141	Windows error event

Si el desplegues, veuràs el log generat per l'antivirus:

Table	JSON
	<pre>{   "_id": "4PGYwH4B9mpedvM6Ziq1",   "_index": "wazuh-alerts-4.x-2022.02.03",   "_score": -1,   "_type": "_doc",   "agent.id": "003",   "agent.ip": "192.168.1.86",   "agent.name": "CETI13",   "data.win.eventdata.data": {     "Kaspersky Endpoint Security for Windows (11.4.0.233) (File Threat Protection)": {       "Result": "Detected: EICAR-Test-File",       "User": "CETI13\\super (Active user)",       "Object": "C:\\Users\\super\\Downloads\\eicar.com",       "Reason": "Expert analysis Database release date: 3/2/2022 10:14:00",       "Hash": "275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f"     }   },   "data.win.system.channel": "Kaspersky Event Log",   "data.win.system.computer": "CETI13" }</pre>

## Windows Defender

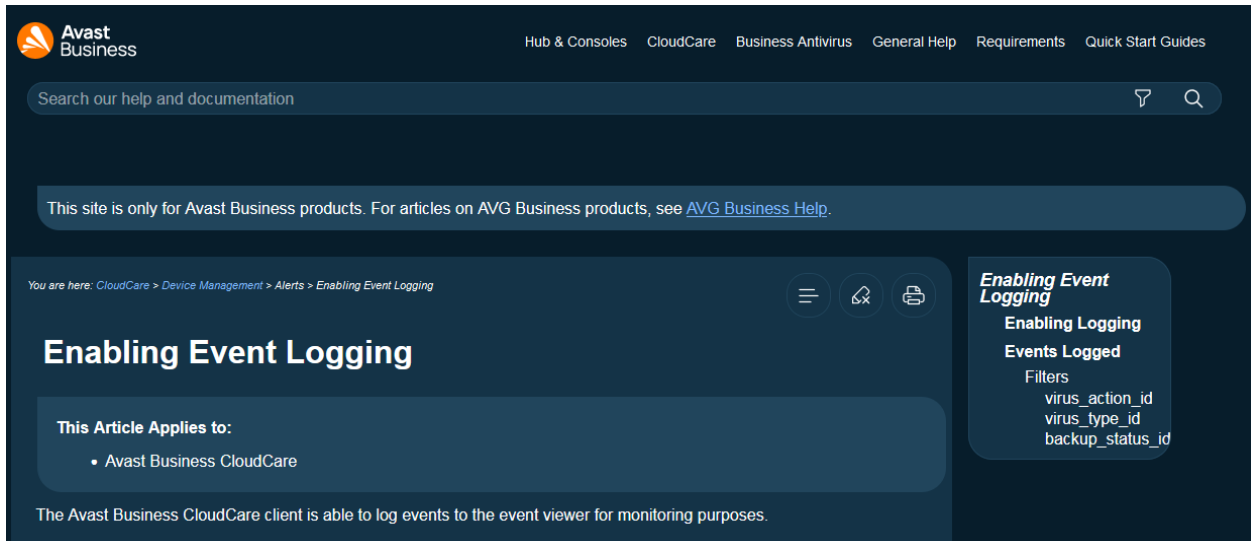
Per a l'antivirus Windows Defender, la directriu és aquesta:

```
<localfile>  
    <location>Microsoft-Windows-Windows Defender/Operational</location>  
    <log_format>eventchannel</log_format>  
</localfile>
```

---

## Avast

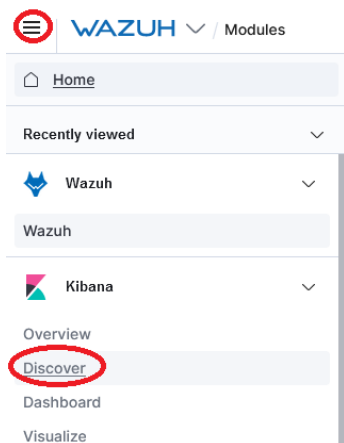
No he sabut trobar la manera de recollir els logs de l'Avast versió gratuïta. Sembla que sí es pot a la versió Avast Business.



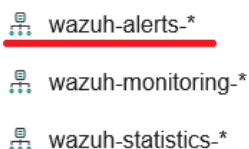
The screenshot shows the Avast Business help center interface. At the top, there's a navigation bar with links: Hub & Consoles, CloudCare, Business Antivirus, General Help, Requirements, and Quick Start Guides. Below this is a search bar with the placeholder text 'Search our help and documentation'. A message states: 'This site is only for Avast Business products. For articles on AVG Business products, see [AVG Business Help](#).' The main content area has a breadcrumb trail: 'You are here: CloudCare > Device Management > Alerts > Enabling Event Logging'. The article title is 'Enabling Event Logging'. Below the title, it says 'This Article Applies to:' followed by a bullet point: 'Avast Business CloudCare'. A note at the bottom states: 'The Avast Business CloudCare client is able to log events to the event viewer for monitoring purposes.' On the right side, there's a sidebar with the title 'Enabling Event Logging' and a section 'Events Logged' with a 'Filters' list containing: 'virus\_action\_id', 'virus\_type\_id', and 'backup\_status\_id'.

## Kibana: Creació d'una cerca per a les alertes dels antivirus

Selecciona l'eina *Discover* de Kibana del menú desplegable:



Si et pregunta l'origen de dades selecciona *wazuh-alerts*-\*

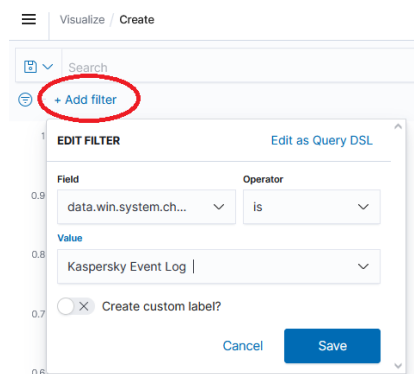


Afegeix un filtre:

*Field: data.win.system.chanel*

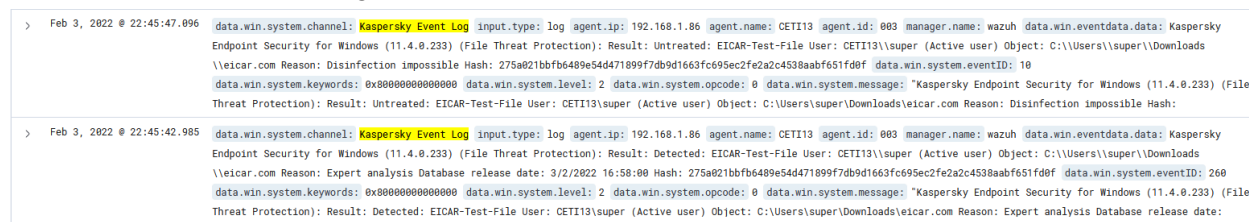
*Operator: is*

*Value: Kaspersky Event Log*




I desa els canvis.

Ara només et mostra els logs que compleixen aquest filtre:



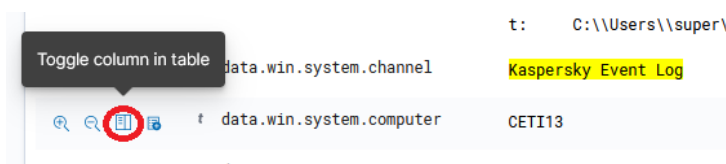
En comptes de veure tota la informació del log, farem una visualització personalitzada amb dues dades: el nom de l'ordinador i la informació de l'alerta.

Desplega l'alerta i veuràs el detall del registre:



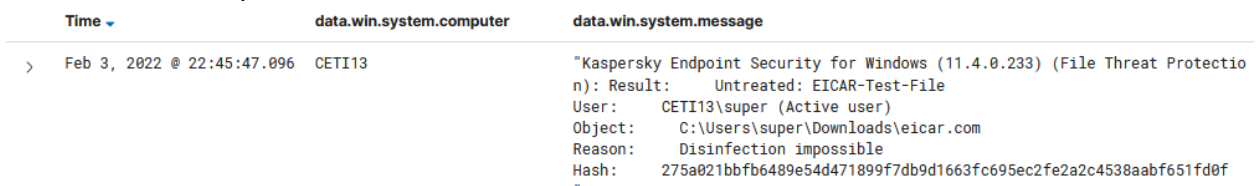
Time	_source
Feb 3, 2022 @ 22:45:47.096	<pre>data.win.system.channel: Kaspersky Event Log Endpoint Security for Windows (11.4.0.233) (F: \\eicar.com Reason: Disinfection impossible H: data.win.system.keywords: 0x8000000000000000 d Threat Protection): Result: Untreated: EICAR-</pre>

Situa el punter del ratolí sobre el camp `data.win.system.computer` i clica l'opció *Toggle column in table*:



Time	data.win.system.computer	data.win.system.message
Feb 3, 2022 @ 22:45:47.096	CETI13	"Kaspersky Endpoint Security for Windows (11.4.0.233) (File Threat Protection): Result: Untreated: EICAR-Test-File User: CETI13\super (Active user) Object: C:\Users\super\Downloads\eicar.com Reason: Disinfection impossible Hash: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"

Desplega un altre cop l'alerta i fes el mateix pel camp `data.win.system.message`  
Ara la informació que ens mostra és més reduïda:

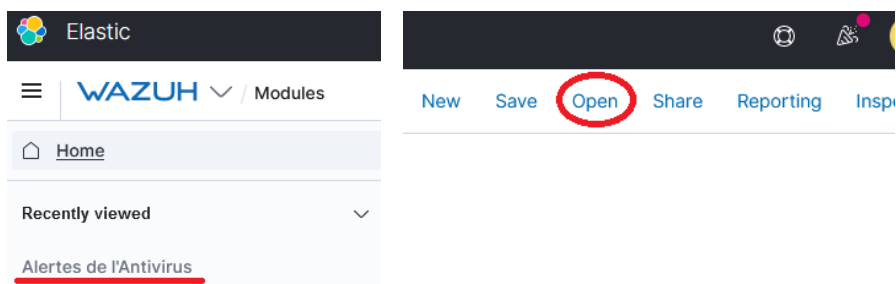


Time	data.win.system.computer	data.win.system.message
> Feb 3, 2022 @ 22:45:47.096	CETI13	"Kaspersky Endpoint Security for Windows (11.4.0.233) (File Threat Protection): Result: Untreated: EICAR-Test-File User: CETI13\super (Active user) Object: C:\Users\super\Downloads\eicar.com Reason: Disinfection impossible Hash: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"

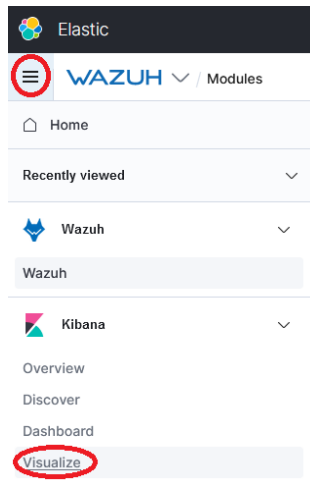
Anomena i desa la cerca:



Ara pots trobar aquesta cerca a les vistes recents i a la barra de menús:



## Kibana: Creació d'una vista sobre la cerca dels antivirus



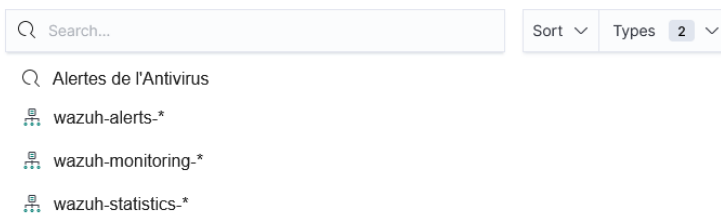
Crea una nova visualització i selecciona un tipus de gràfic, per exemple, de barres verticals:



### Vertical Bar

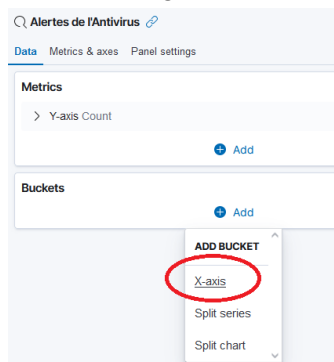
Com a font de dades, selecciona la cerca que acabem de crear: *Alertes de l'Antivirus*

New Vertical Bar / Choose a source

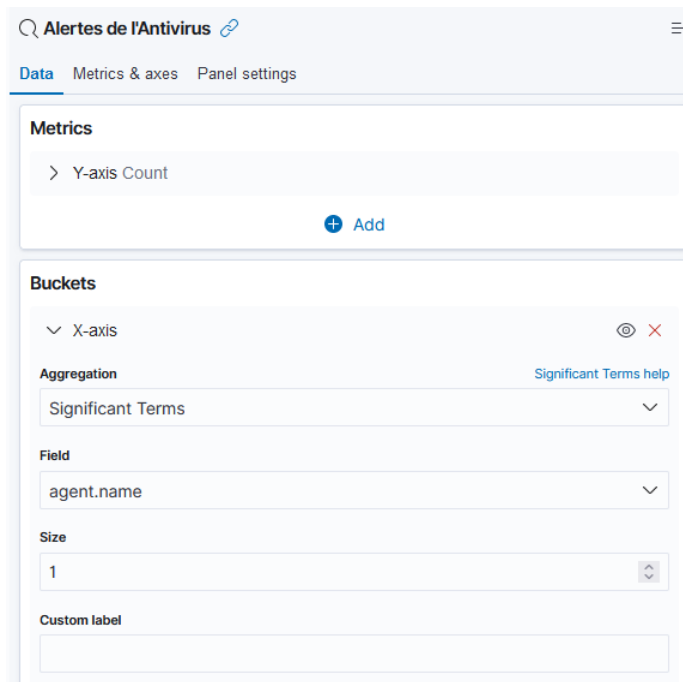


Ara només veus la coordenada vertical amb el número d'alertes. Seria interessant veure a l'eix horitzontal les màquines afectades.

Per això afegeix un X-axis:



I selecciona els paràmetres adequats:



Alertes de l'Antivirus

Data Metrics & axes Panel settings

**Metrics**

> Y-axis Count

+ Add

**Buckets**

▼ X-axis

**Aggregation** Significant Terms help

Significant Terms

**Field**

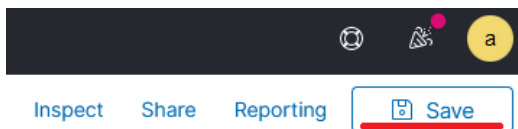
agent.name

**Size**

1

**Custom label**

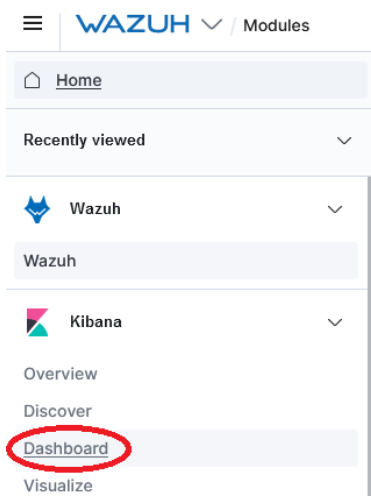
Per acabar, anomena i desa la visualització:



Inspect Share Reporting **Save**

## Creació d'un *dashboard*

Ves a l'apartat de *Dashboard* per crear un panell:



WAZUH / Modules

Home

Recently viewed

Wazuh

Wazuh

Kibana

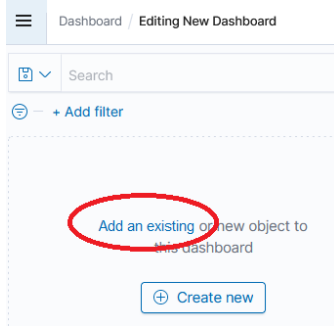
Overview

Discover

**Dashboard**

Visualize

I selecciona un element existent:



I tria la vista que acabes de triar:

Add panels



I desa els canvis.

En el meu cas, com que només tinc alertes d'una sola màquina, el gràfic només té una columna.



Activitat: genera un *dashboard* a partir d'una vista i entrega una captura de la vista i del *dashboard*.