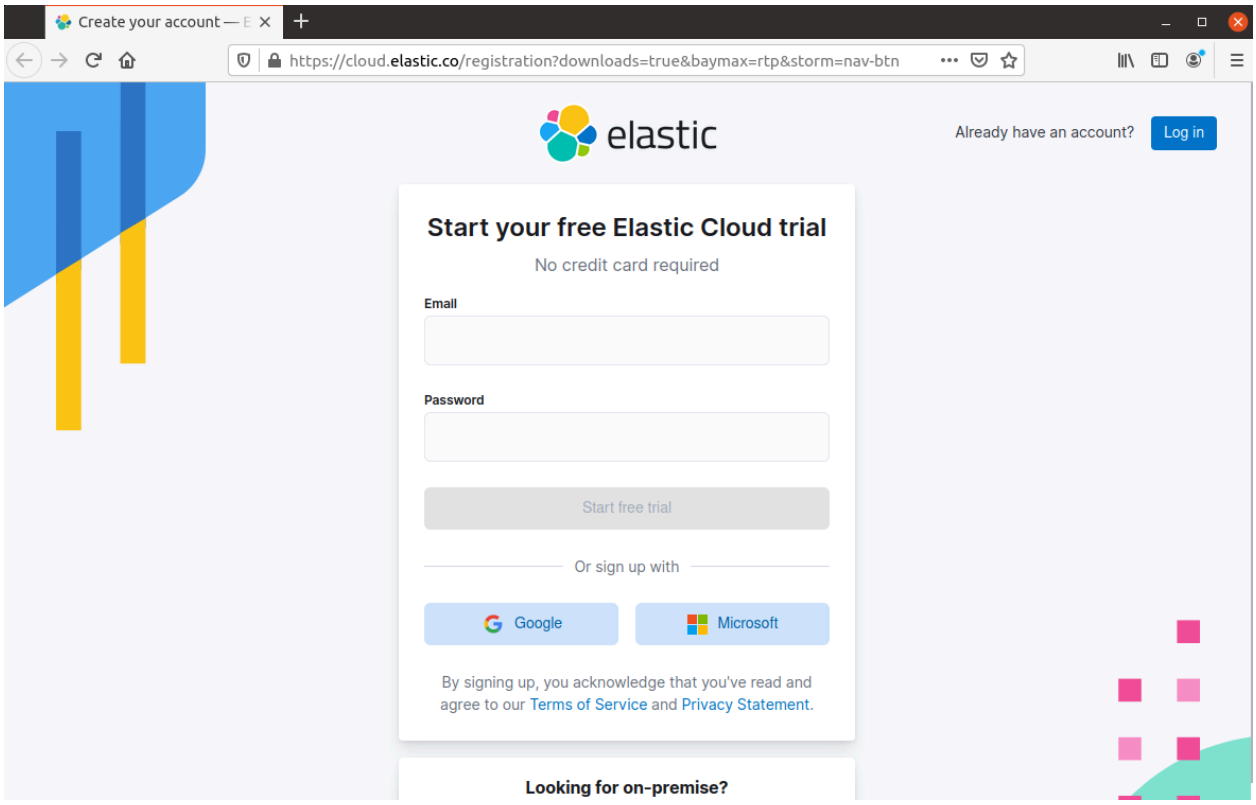
ELK Documentation

This is a document to show the setup of ELK in the cloud:
E - Elasticsearch
L - Logstash
K - Kibana

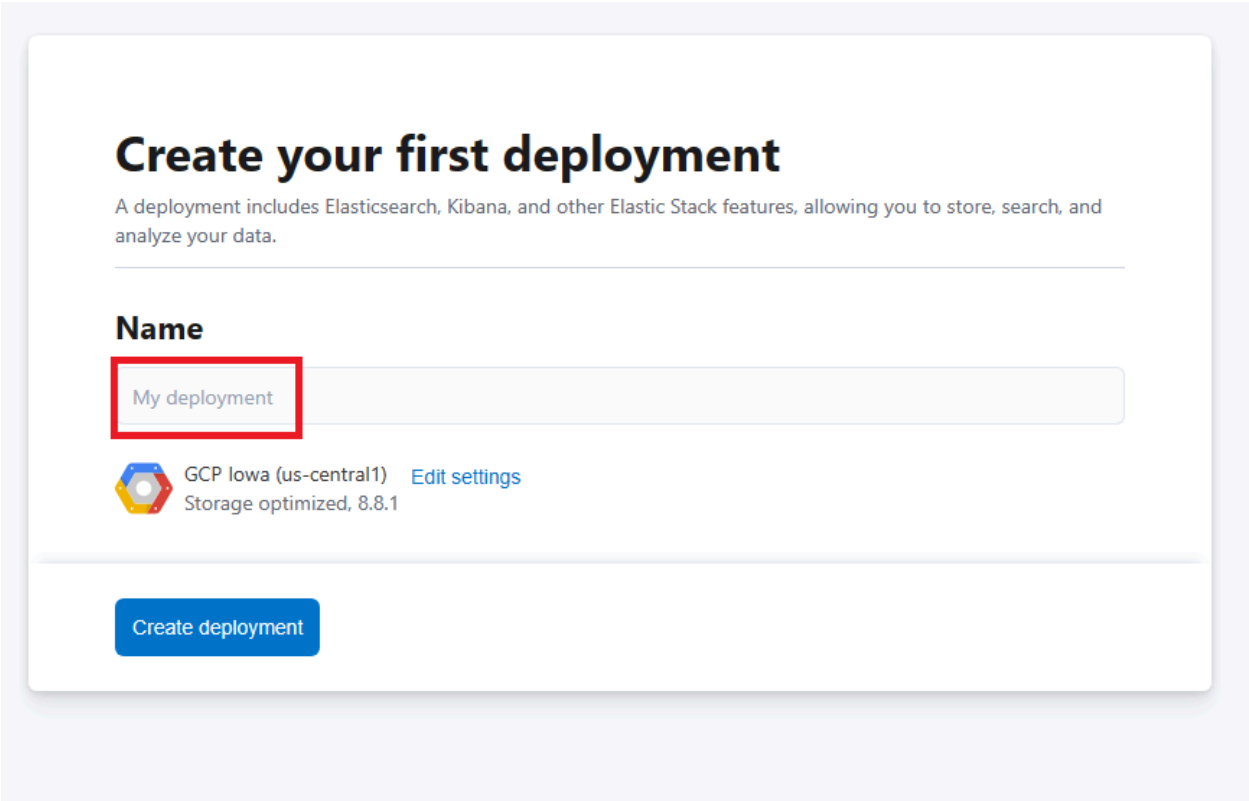
ELK is a SIEM that enables defenders to detect attacks and conduct threat hunting.

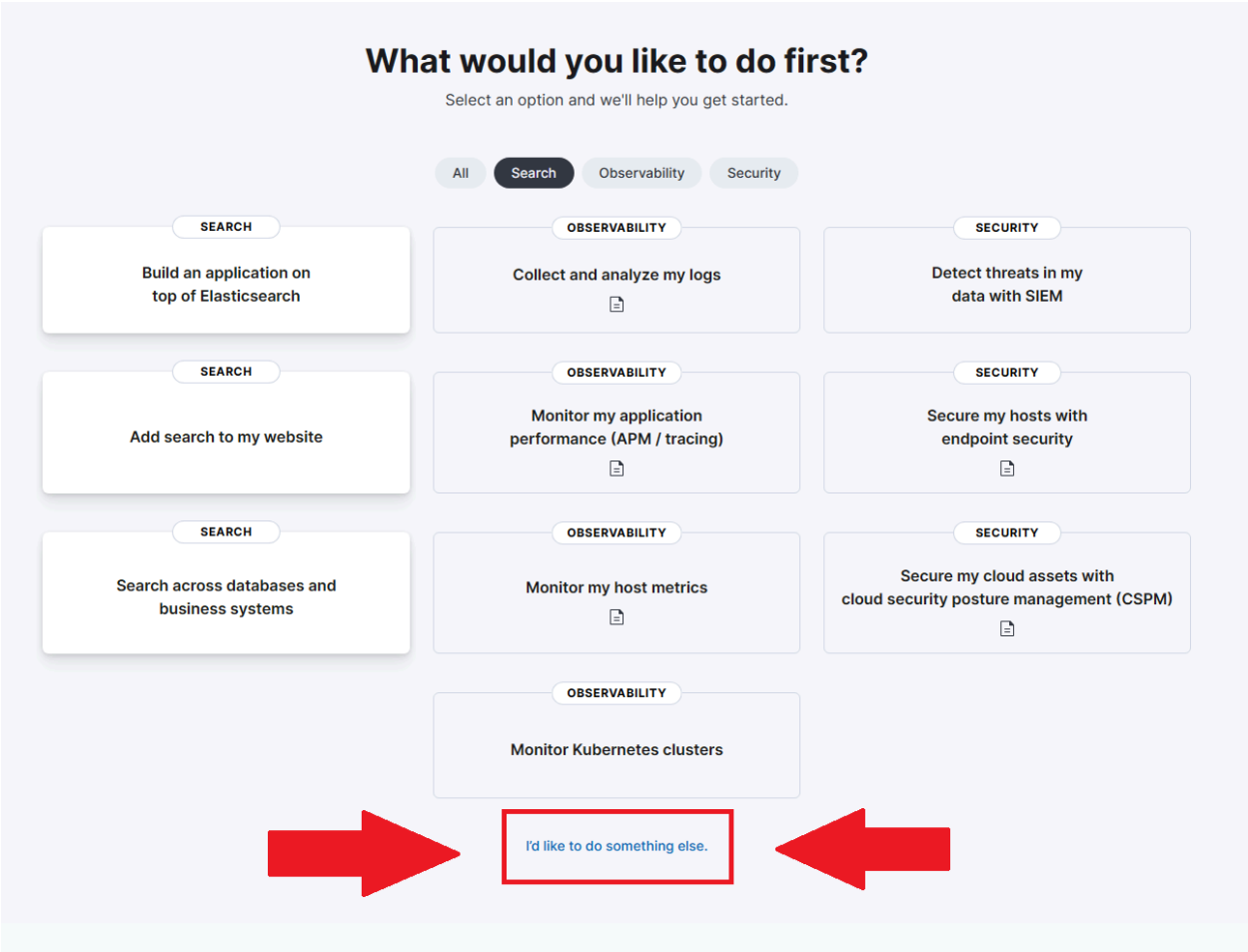
Step 1: Create an account using [this link]



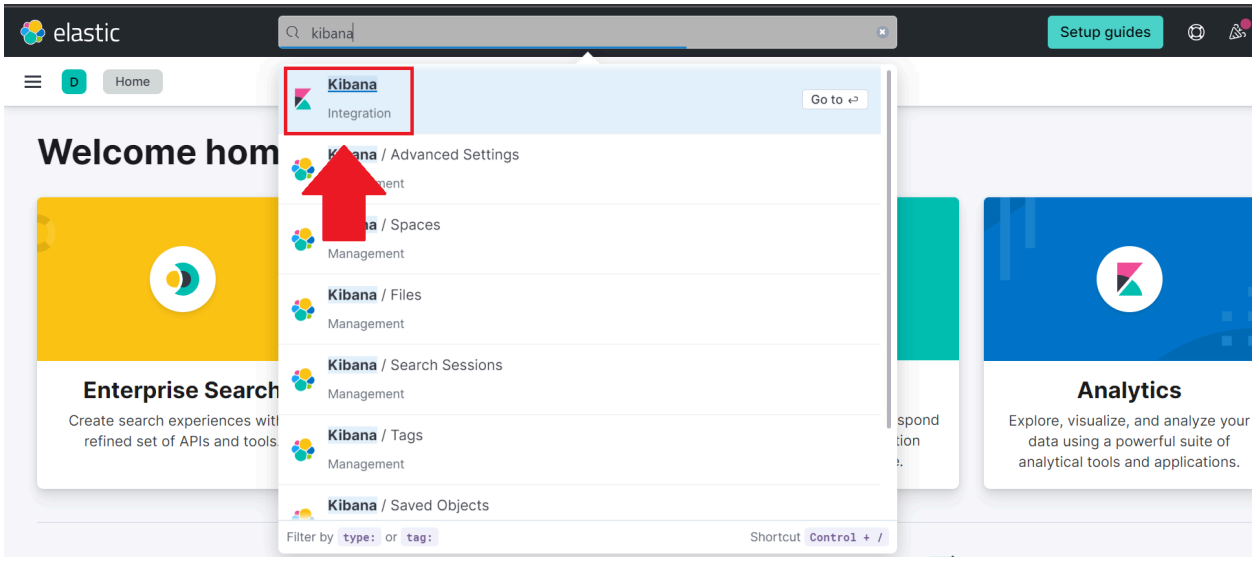
After logging in, fill in all the details and proceed ahead.

Step 2: Create an ELK instance
Give the deployment some name and click “Create Deployment”

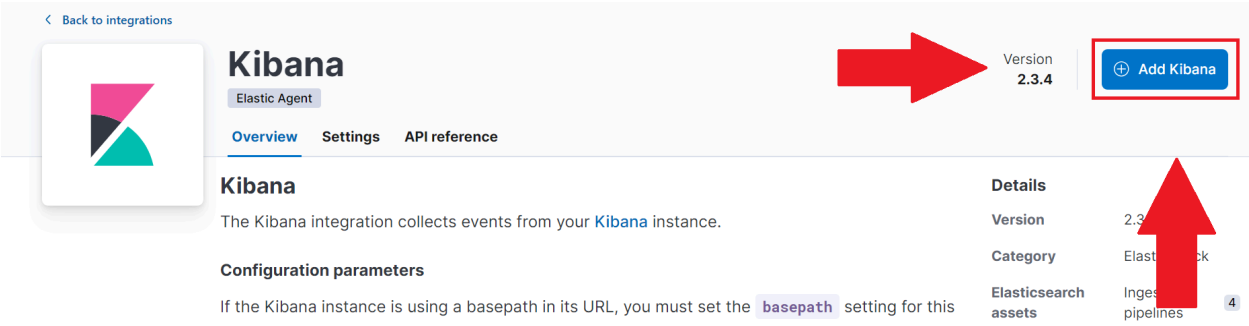




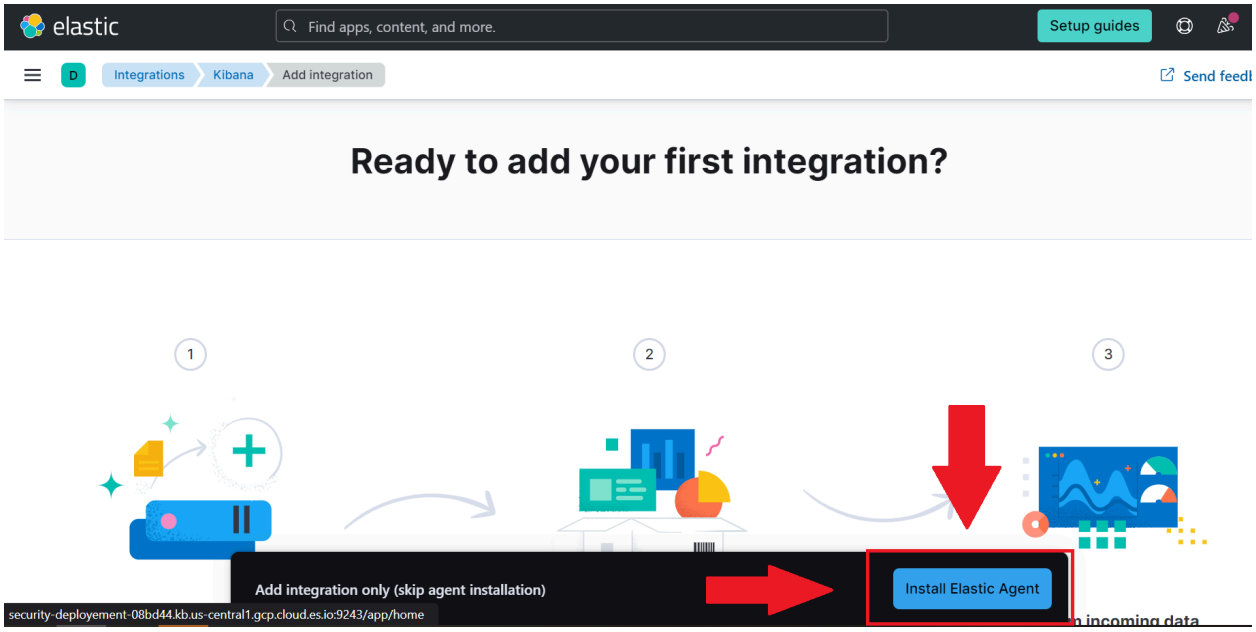
At the top of the search bar, search for “Kibana”



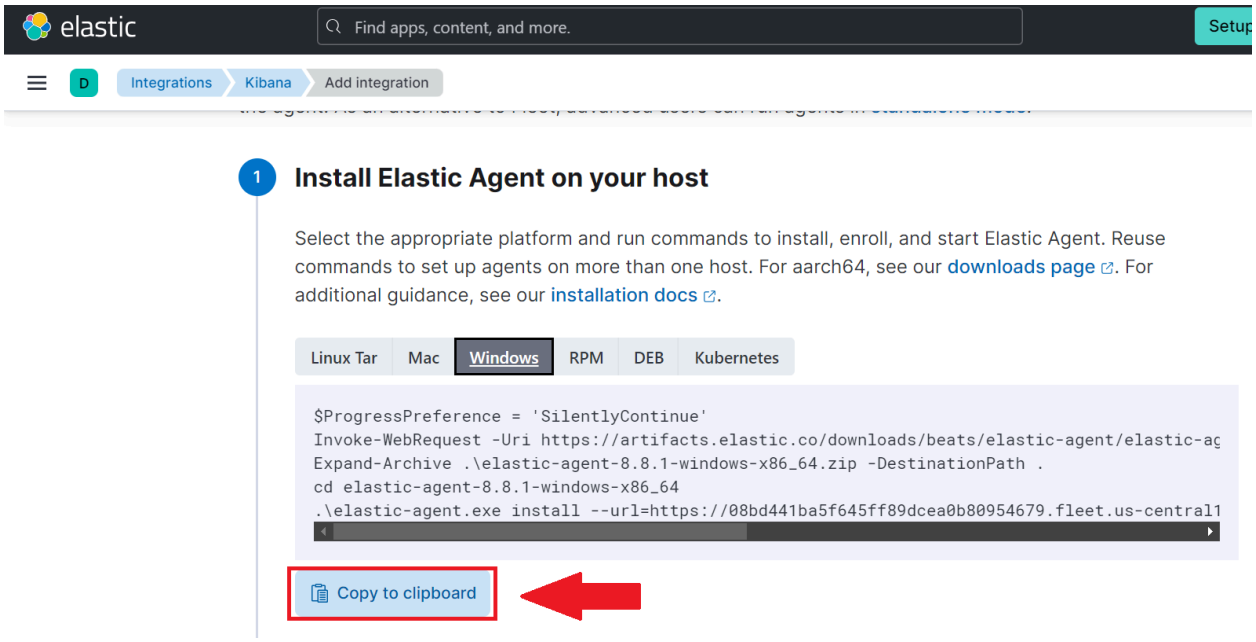
Once Kibana is selected, click on Add Kibana



We will next be prompted to "Install Elastic Agent" This is what we are going to put on our machine that monitors what's happening. Click "Install Elastic Agent"



Next, we add the Elastic Agent to our host machine. I am selecting Windows

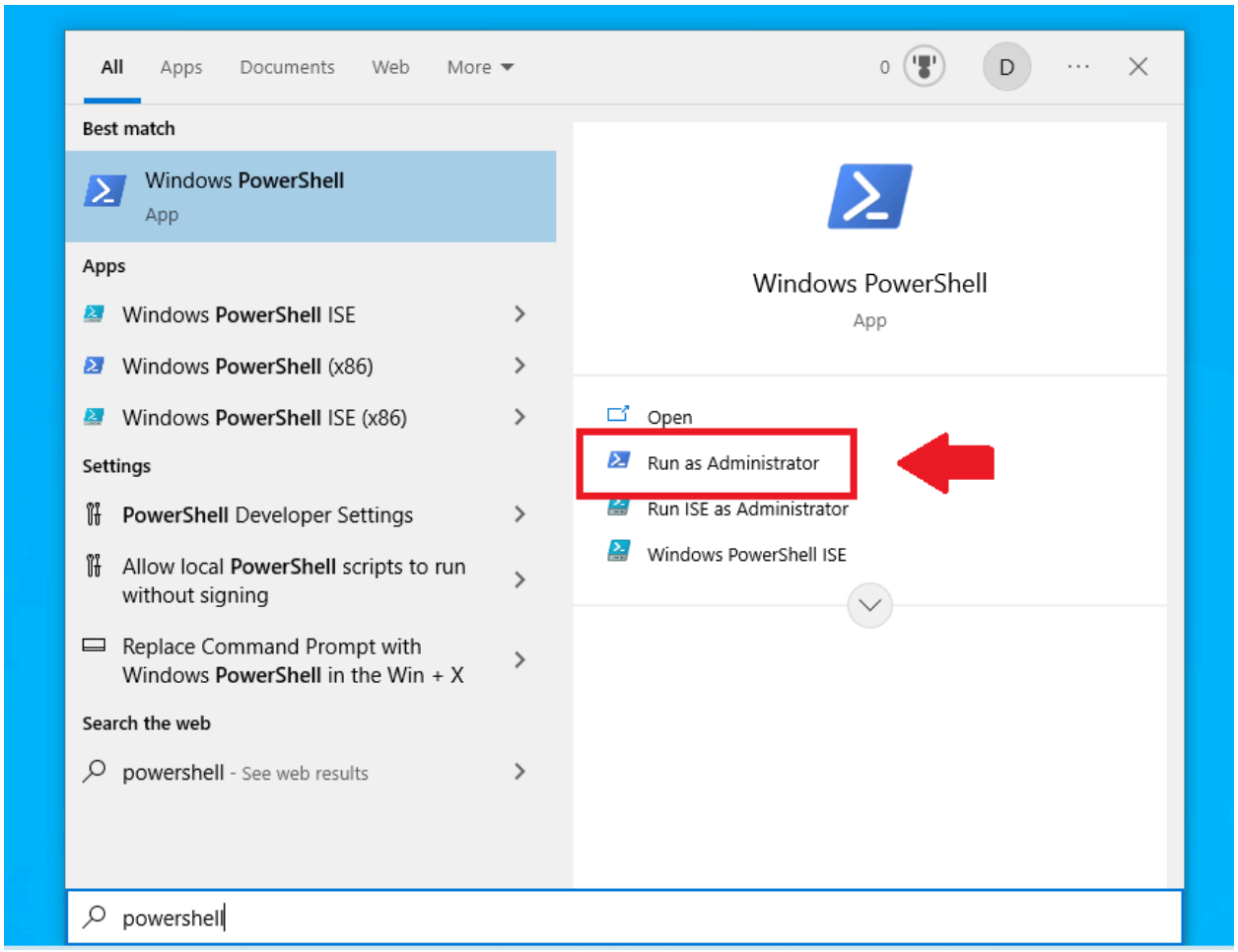


Note: We should hold on to this command because we will be using it in the future. I just saved it in a notepad file called agent.txt

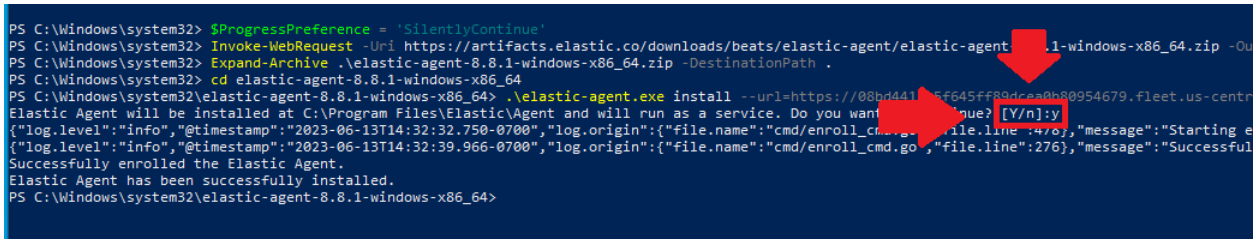
The ELK stack is now configured and we have our connection information saved. Part two will cover how to install and configure an Elastic Agent.

Step 3: Downloading the Elastic Agent

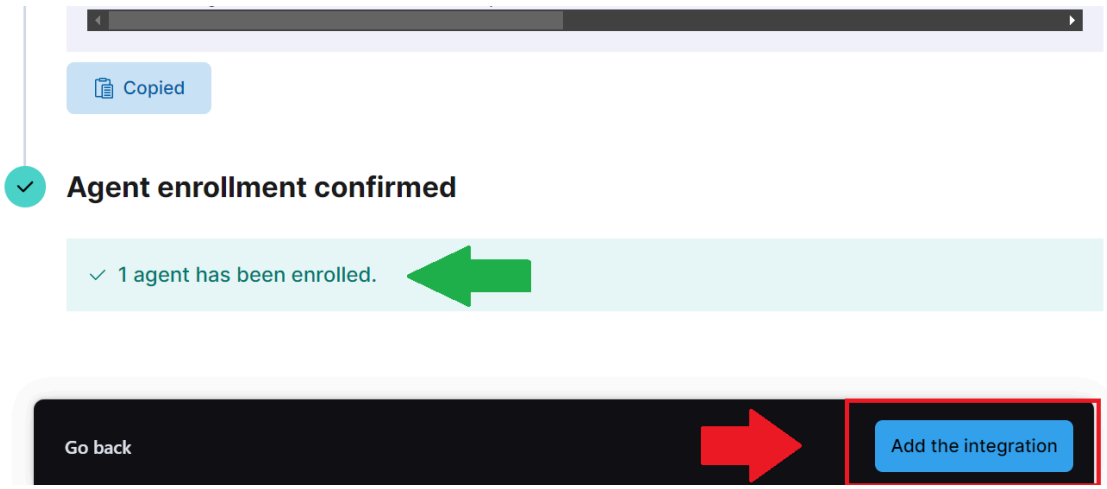
Press the Windows button search “Powershell” and run it as administer



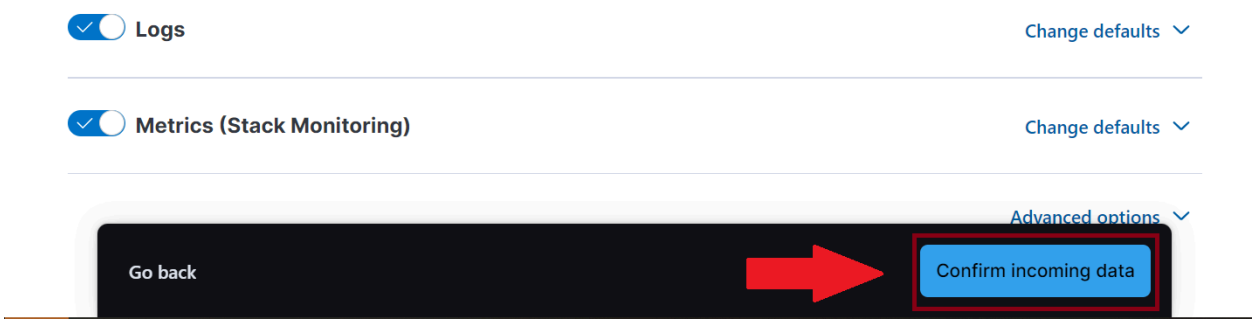
Once PowerShell is opened, copy and paste the agent information that we have copied one by one. Enter “Y” wherever prompted



Go back to the browser and you can see “1 agent has been enrolled” click on “Add the integration”

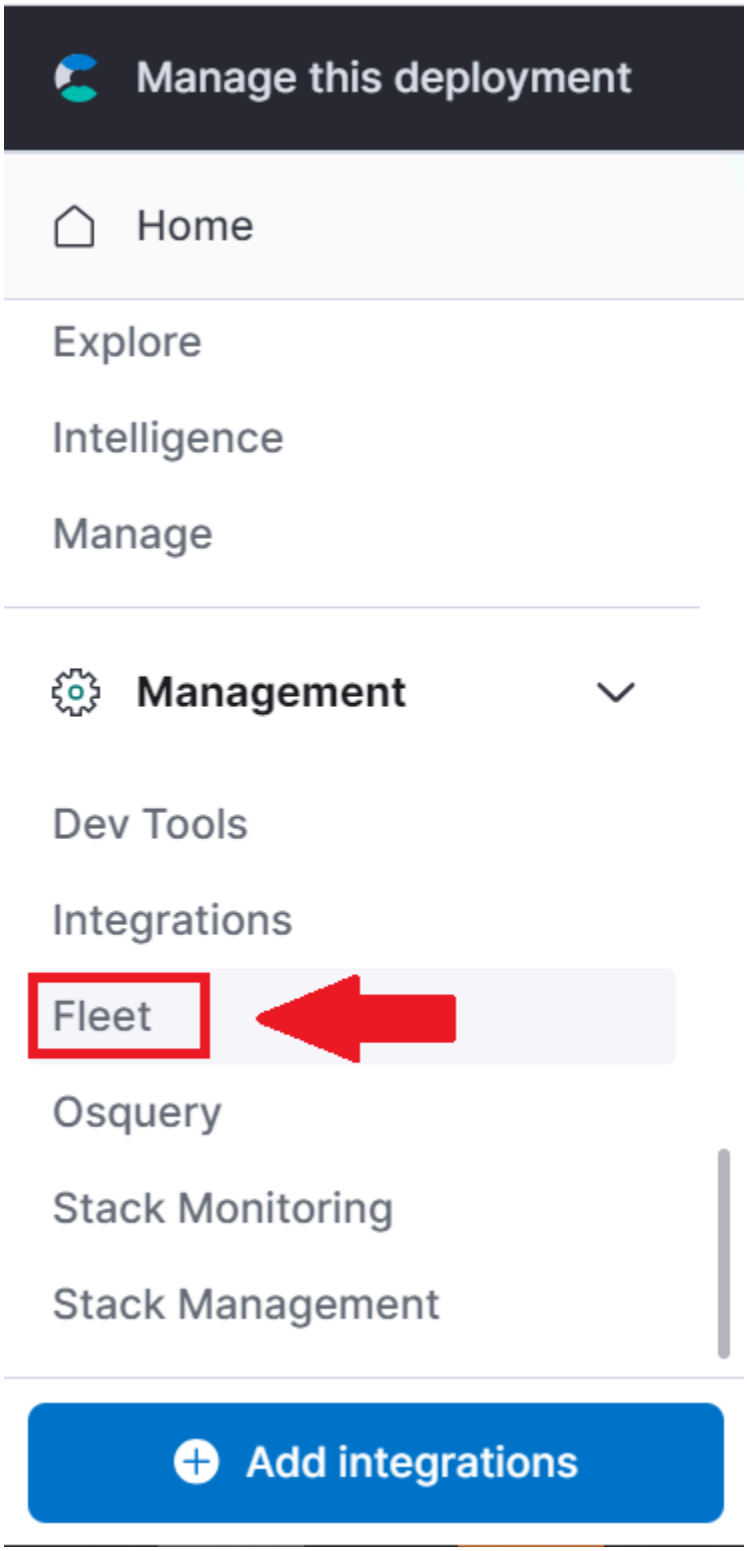


On the next page leave everything default and click "Confirm Incoming Data".

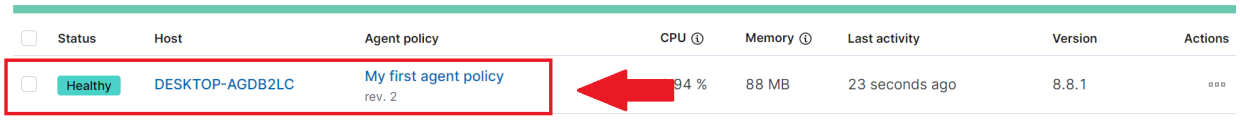


The browser will take a few seconds to confirm the machine is connected, once thats finished click "View Assets"

Step 4: Check the Fleet
Go to the hamburger menu, navigate to Management, and click on “Fleet”



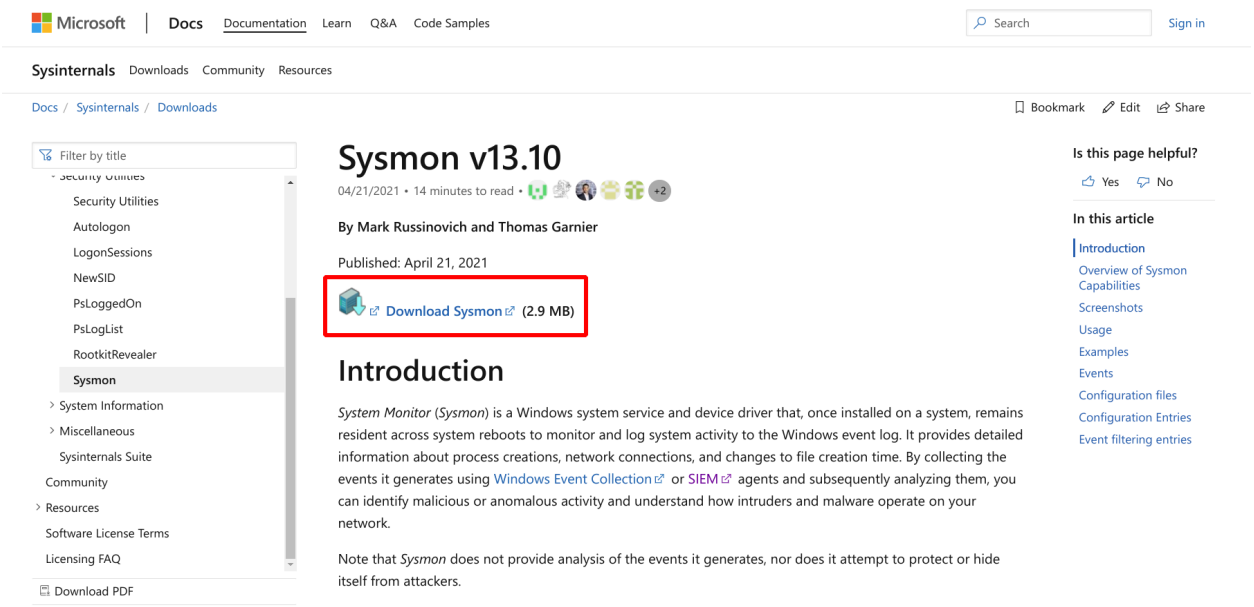
Make sure that the device is connected



Our Elastic Agent is installed and configured to be connected to our ELK instance in the cloud.

Step 5: Download Sysmon

Use [this link](#) to download Sysmon



Once downloaded, extract the contents to the Downloads folder

After it's done, click on the Windows icon type "Powershell" and run it as administrator.

In your PowerShell window, enter the following command. You will need to substitute [USER] for the user you are using on your local system.

cd C:\Users\[USER]\Downloads\Sysmon

The following command will install and start Sysmon as a service.

.\Sysmon.exe -i -n -accepteula

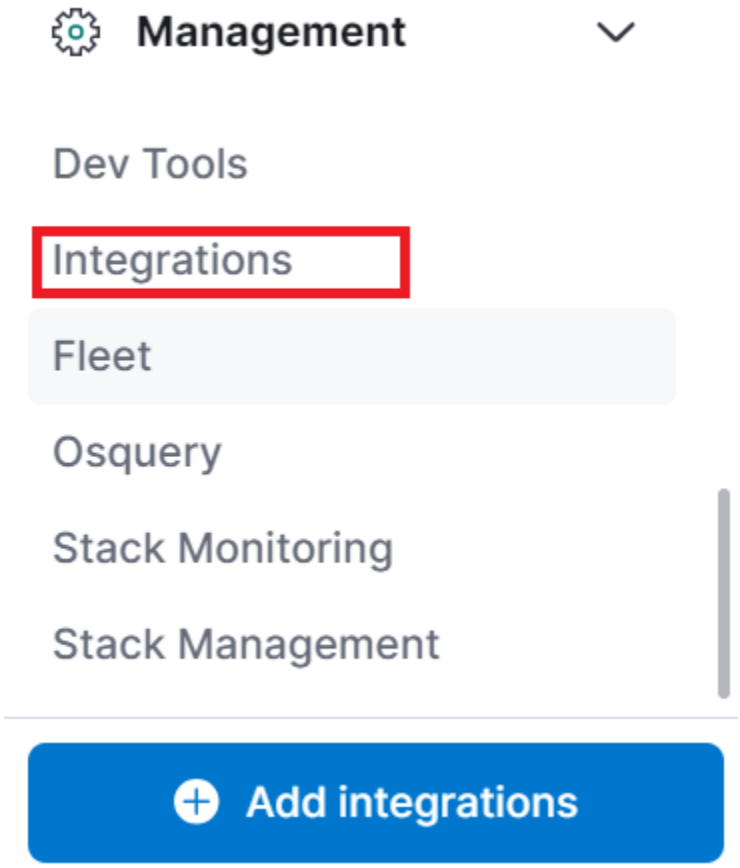
The output would look like this:

```
PS C:\Windows\system32> cd C:\Users\Chris\Downloads\Sysmon
PS C:\Users\Chris\Downloads\Sysmon> .\Sysmon.exe -i -n -acceptula


System Monitor v15.12 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install:                Sysmon.exe -i [<configfile>]
Update configuration:   Sysmon.exe -c [<configfile>]
Install event manifest: Sysmon.exe -m
Print schema:           Sysmon.exe -s
Uninstall:              Sysmon.exe -u [force]
  -c   Update configuration of an installed Sysmon driver or dump the
       current configuration if no other argument is provided. Optionally
       take a configuration file.
  -i   Install service and driver. Optionally take a configuration file.
  -m   Install the event manifest (done on service install as well)).
  -s   Print configuration schema definition of the specified version.
       Specify 'all' to dump all schema versions (default is latest)).
  -u   Uninstall service and driver. Adding force causes uninstall to proceed
       even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.

PS C:\Users\Chris\Downloads\Sysmon>
```

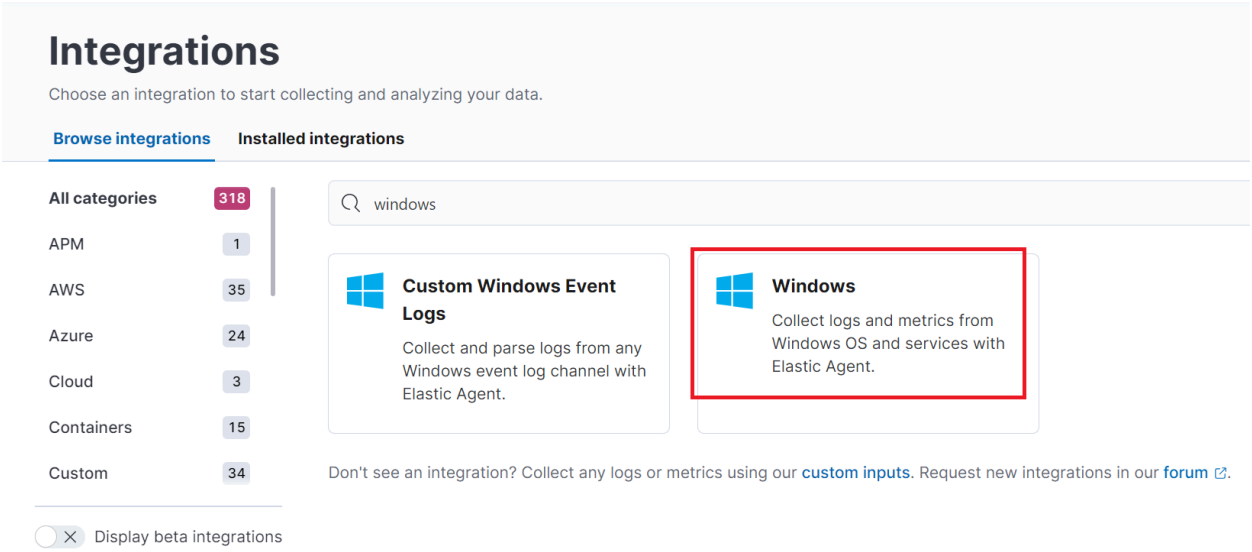
Now that Sysmon is running on our system, we need to configure our Elastic agent to gather these logs. Sign into your cloud account.

[Elastic Cloud Login]

Navigate to "Integrations" through the navigation menu.

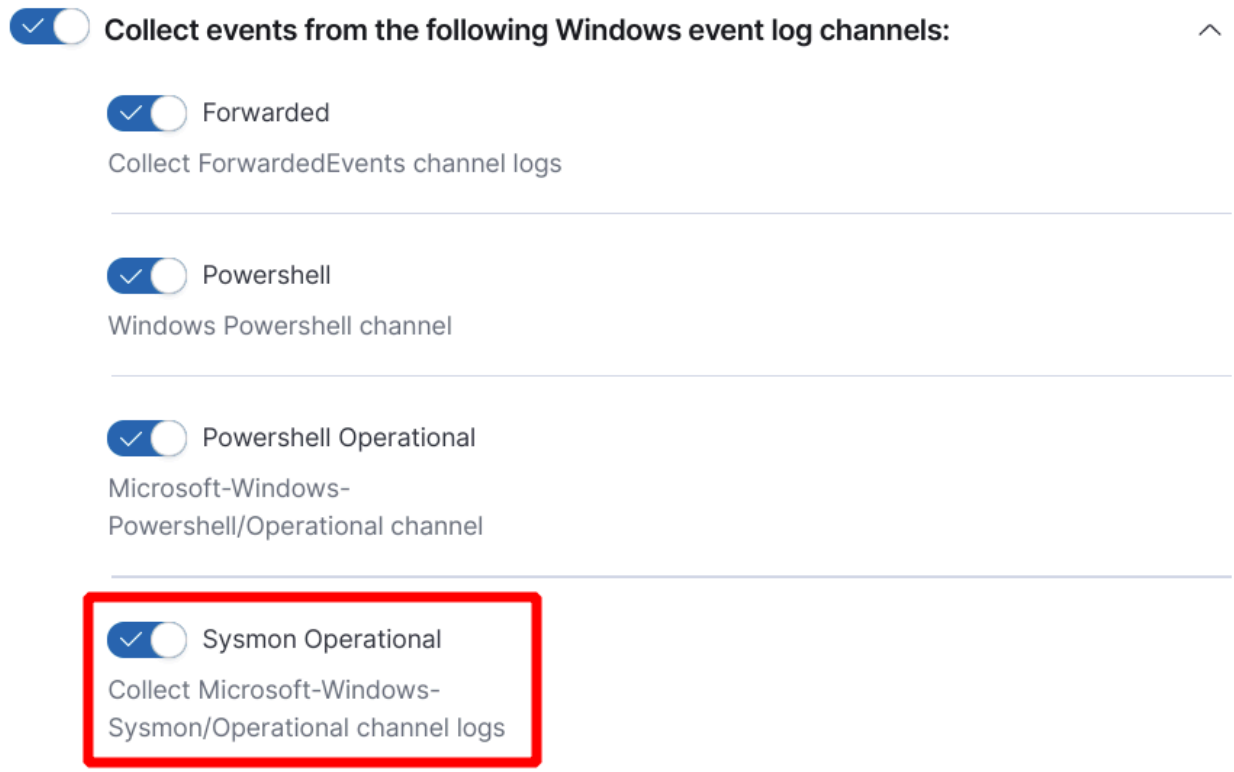


At the top of the page enter "windows" into the search bar. Select “Windows”



Add the Windows Integration

By default, the Sysmon logs channel should be active. This can be checked under the "Collect events from the following Windows event log channels:" section of the "Add Integration" page.

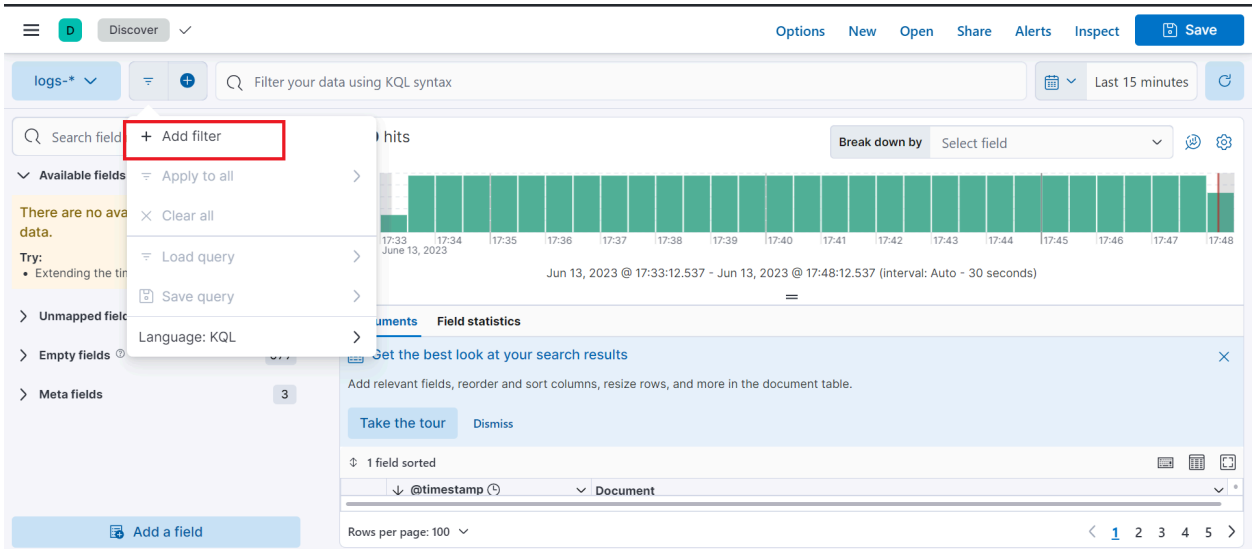


Click Save and Continue

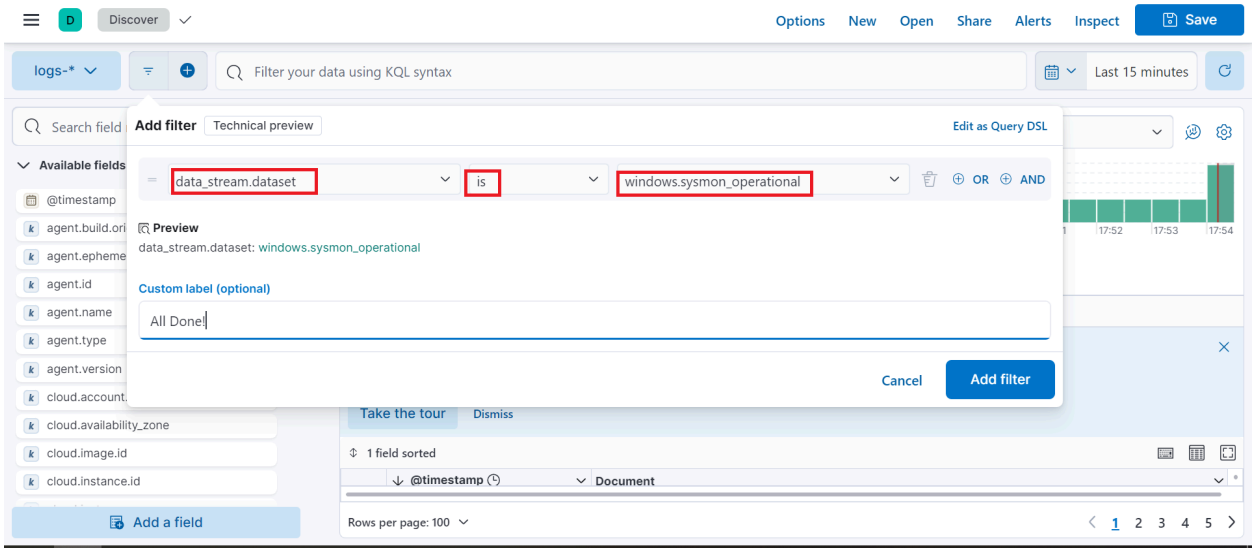
When prompted click "Add elastic agent to your hosts".

Now that we've configured the ELK in the cloud, play around and make some log activities like making a few Google searches, adding files, deleting files, moving files, etc.

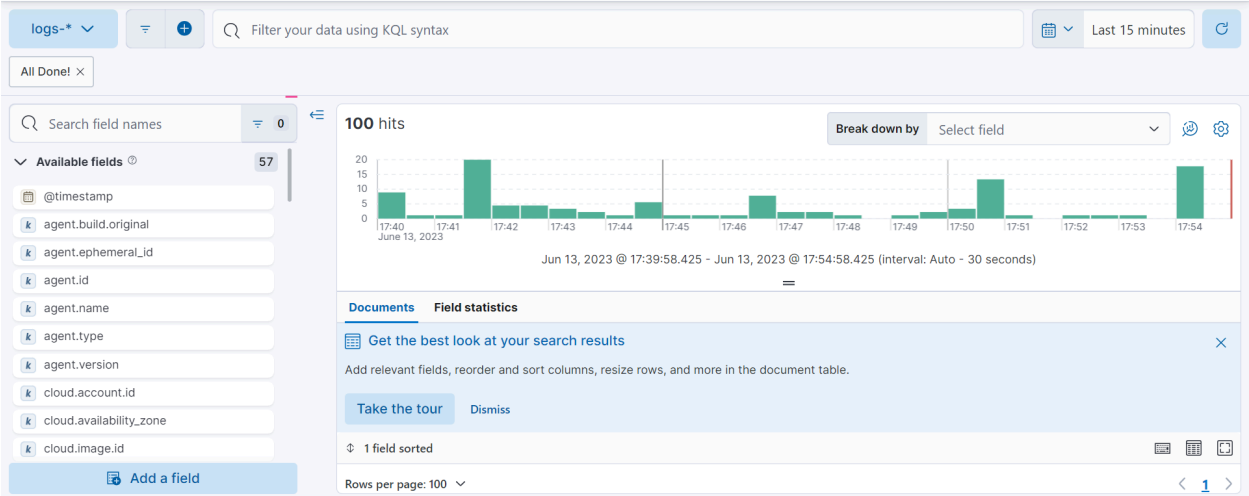
After you have created some log activity, navigate to "Discover" by accessing the hamburger menu on the top left.



Set a filter on your data to limit your results to sysmon data. This can be done by searching the "data_stream.dataset" field for "windows.sysmon_operational" data. Then click "add filter". Your filter should now be set.



If you have a result and not an error, your Sysmon data is being collected and sent to Elastic.



Note: I have only used the Elasticsearch and Kibana of ELK and the Logstash isn't being implemented