Security Workshop 101

Contents

Preparing for the Labs

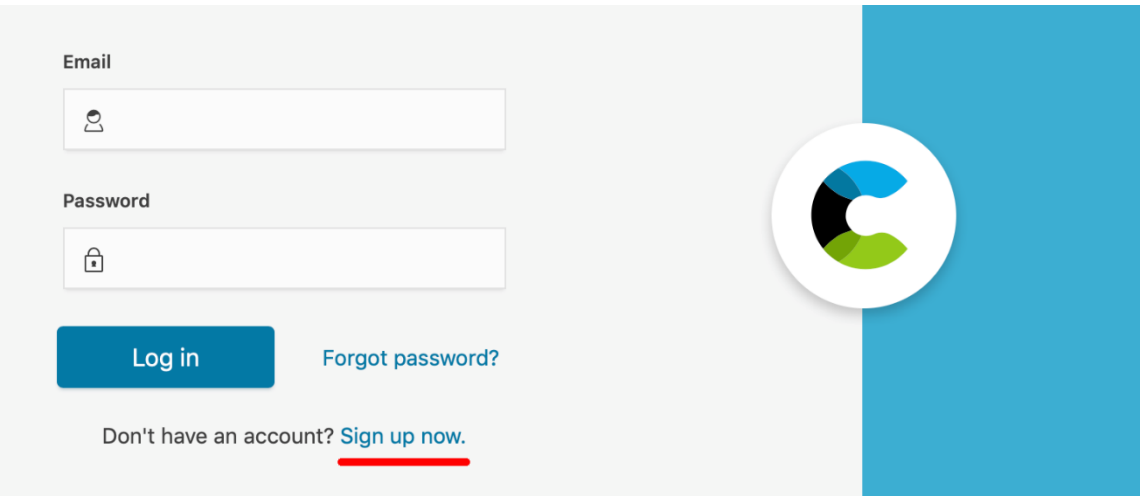
1. All of the documentation and commands are located at https://github.com/NeilADesai/Sec101Workshop.

2. If you plan on copy/pasting the commands, instead of typing them use the associated text files located in the above repository.

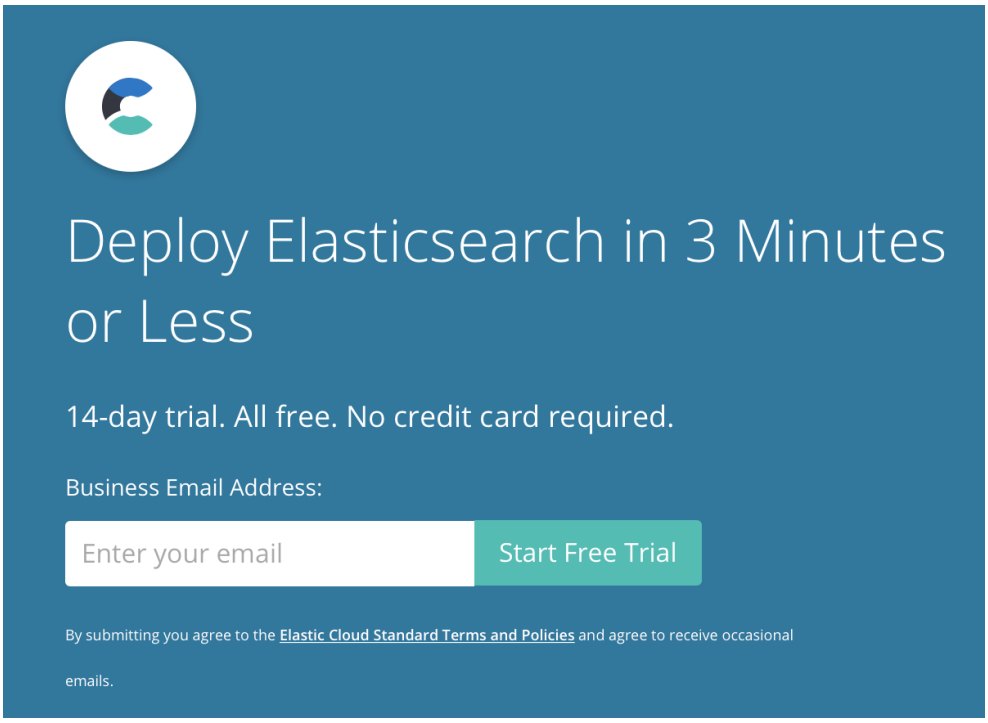
3. Copy/paste to the Windows host can be problematic. Using a browser inside the Windows lab environment browse to the repository and copy/paste from within the VM itself.

Creating an Elasticsearch Cluster in Elastic Cloud (Lab 1)

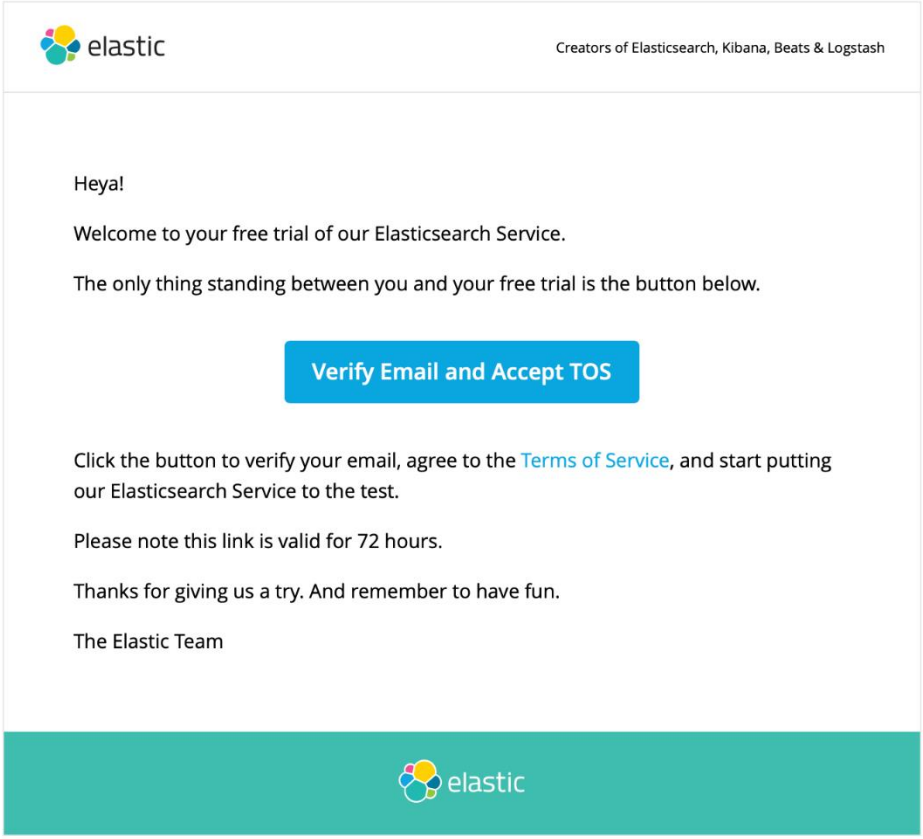
1. Sign up for the Elastic Cloud Trial
    a. Visit https://cloud.elastic.co and click "Sign up now"



    b. Enter your business email (no credit card is required). The cluster you build will be hosted for free for 14 days.



    c. Check your email to verify your account.



elastic

Creators of Elasticsearch, Kibana, Beats & Logstash

Heya!

Welcome to your free trial of our Elasticsearch Service.

The only thing standing between you and your free trial is the button below.

Verify Email and Accept TOS

Click the button to verify your email, agree to the Terms of Service, and start putting our Elasticsearch Service to the test.

Please note this link is valid for 72 hours.

Thanks for giving us a try. And remember to have fun.

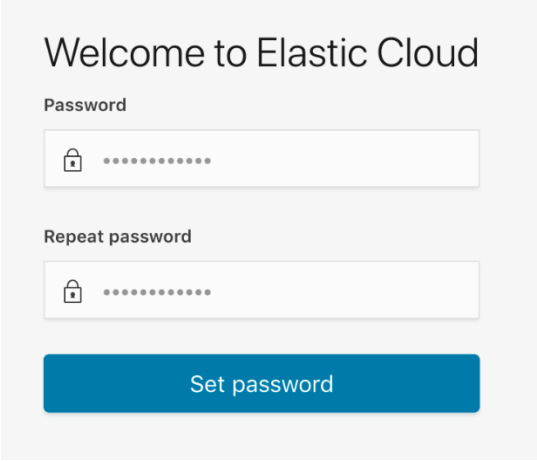
The Elastic Team

elastic

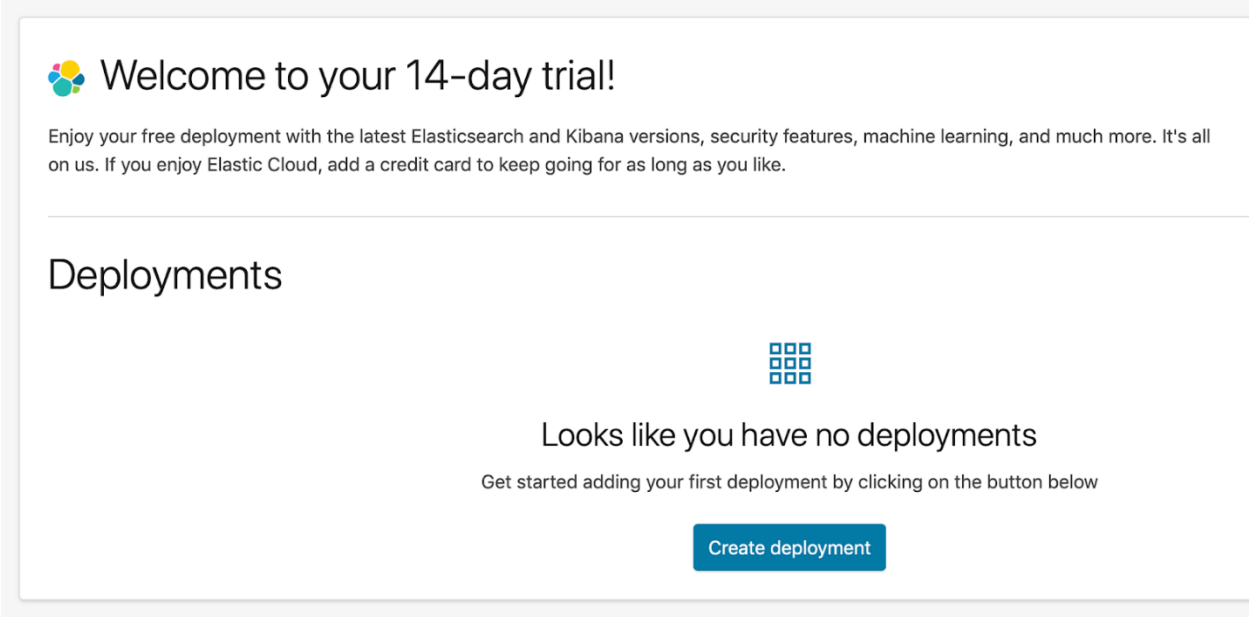
d. Log in and give your account a strong password.

   i. Note: The form will have what looks like a password already filled in. Click the input box, and it will disappear. Enter a new strong password to secure your account.

Tip: You will have a total of 3 passwords to manage in this lab. They will all be different. Securely note them somewhere so you can easily copy & paste them as needed

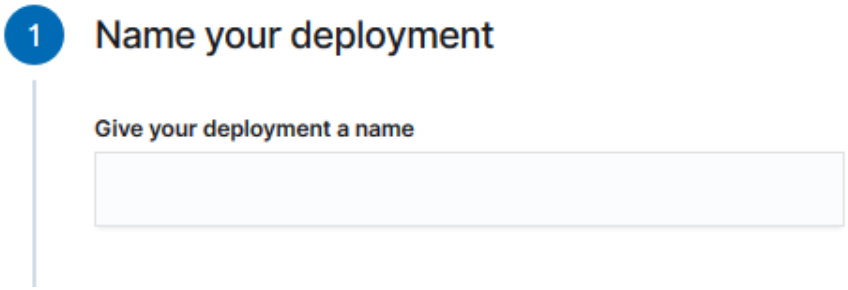


e. You should now be looking at the dashboard.

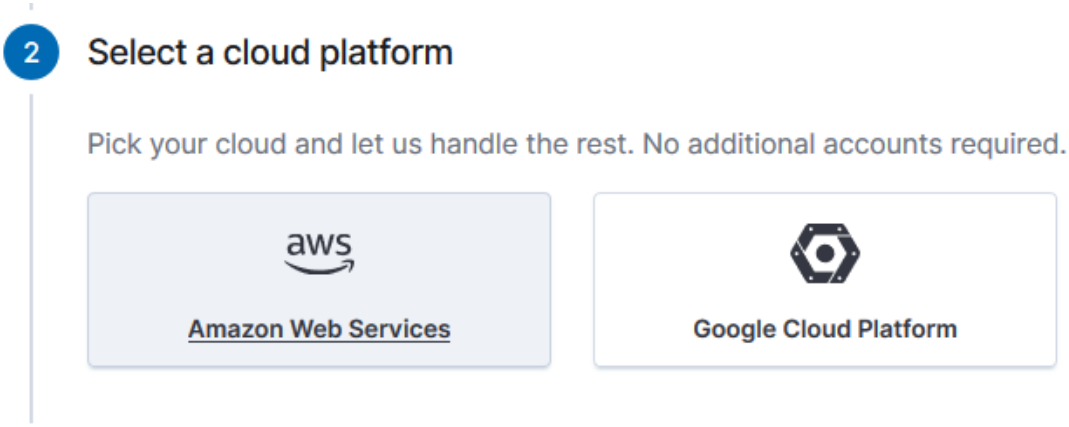


f. Click “Create deployment.”

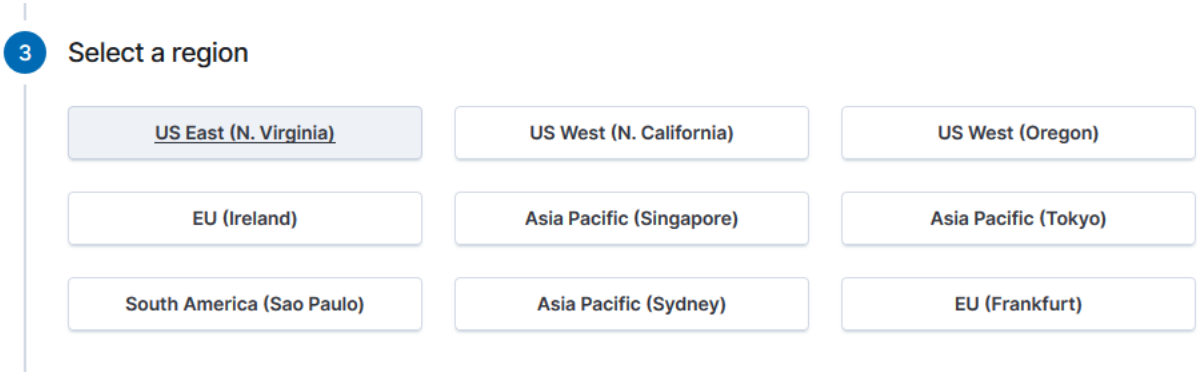
i. Give your deployment at name



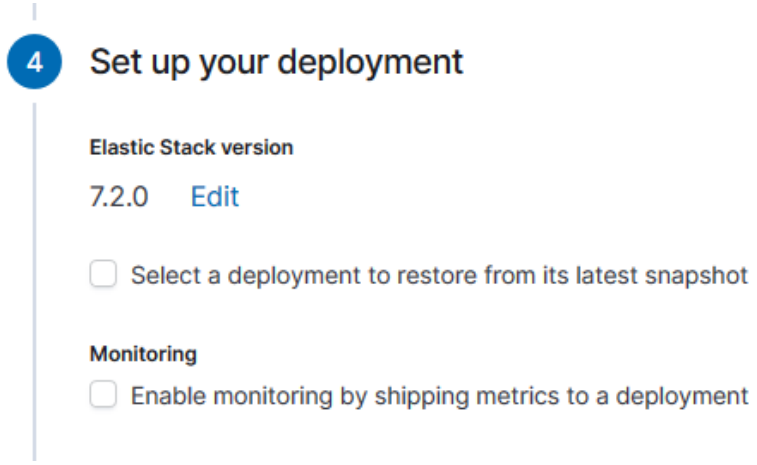
g. Select a Cloud Platform



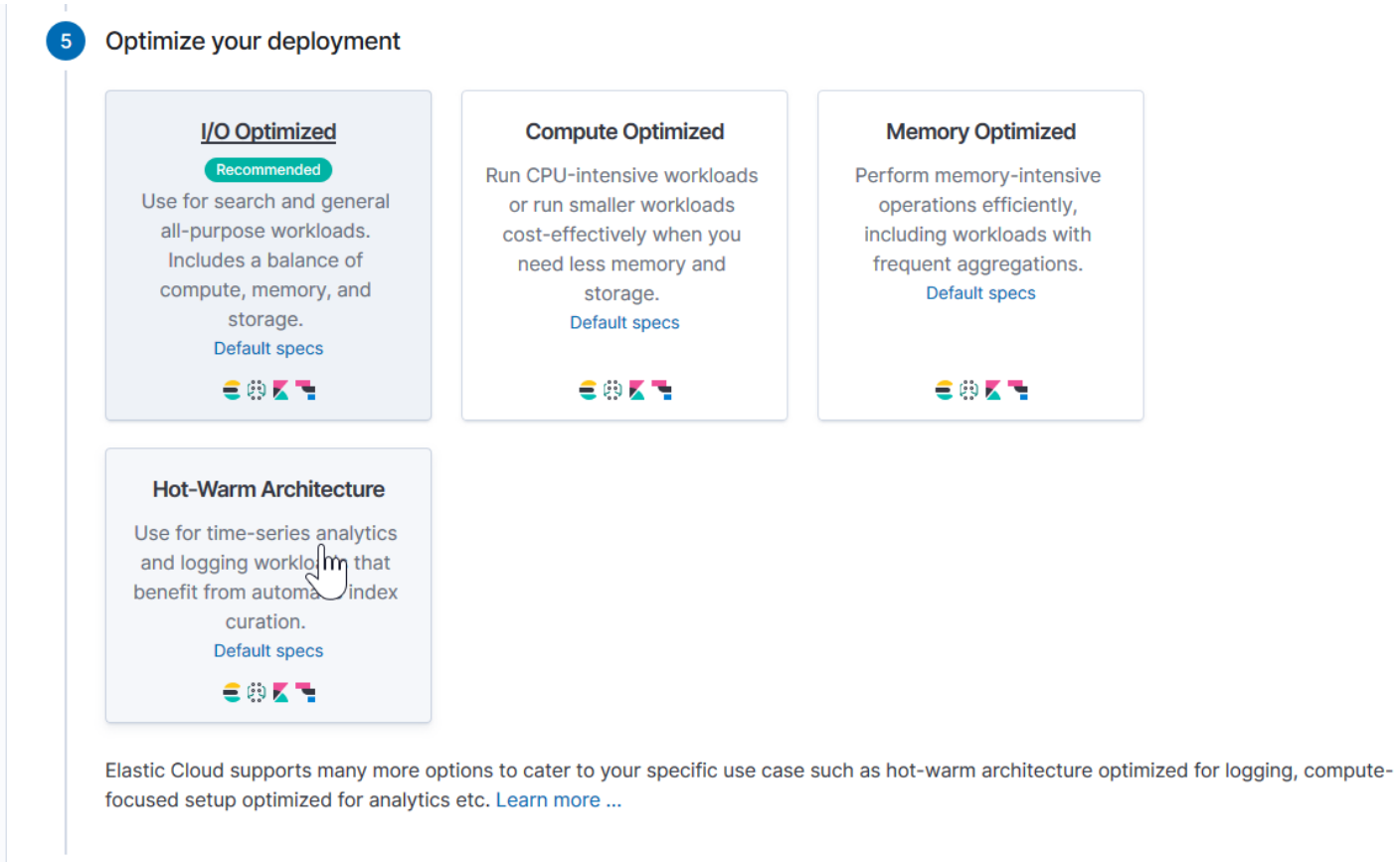
h. Select a region



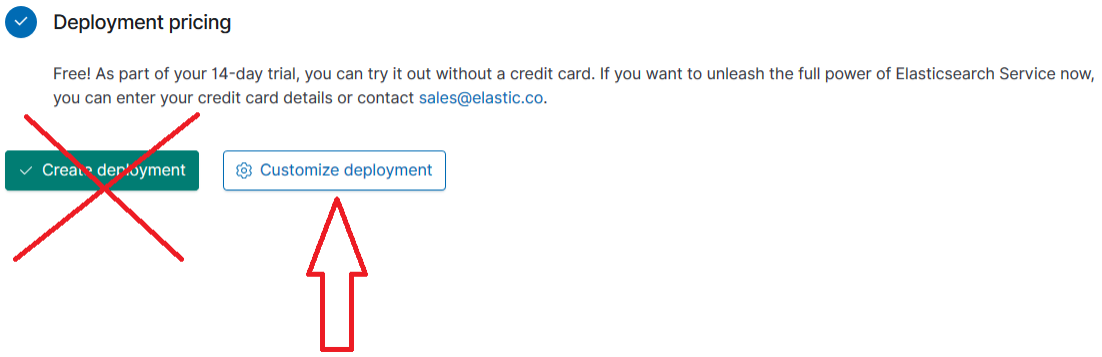
i. Set up your deployment. Chose version 7.2.0



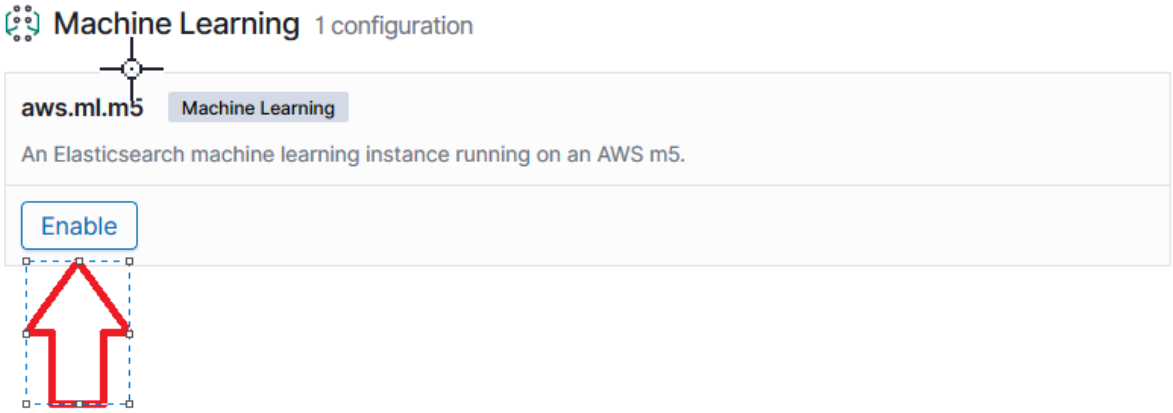
j. Optimize your deployment. Choose “I/O Optimized”



k. At “Deployment Pricing” choose “Customize deployment”

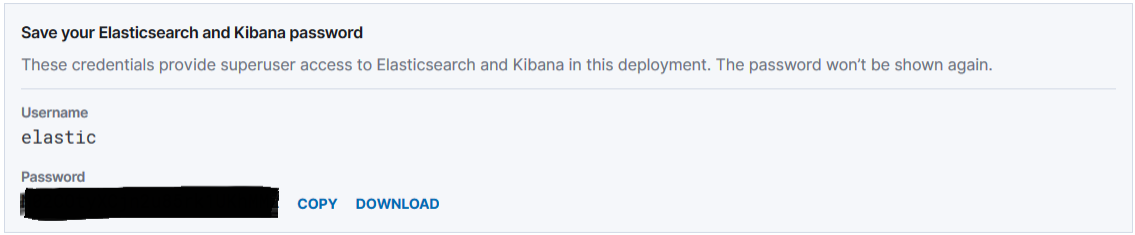


l. Look for “Machine Learning” and click “Enable”

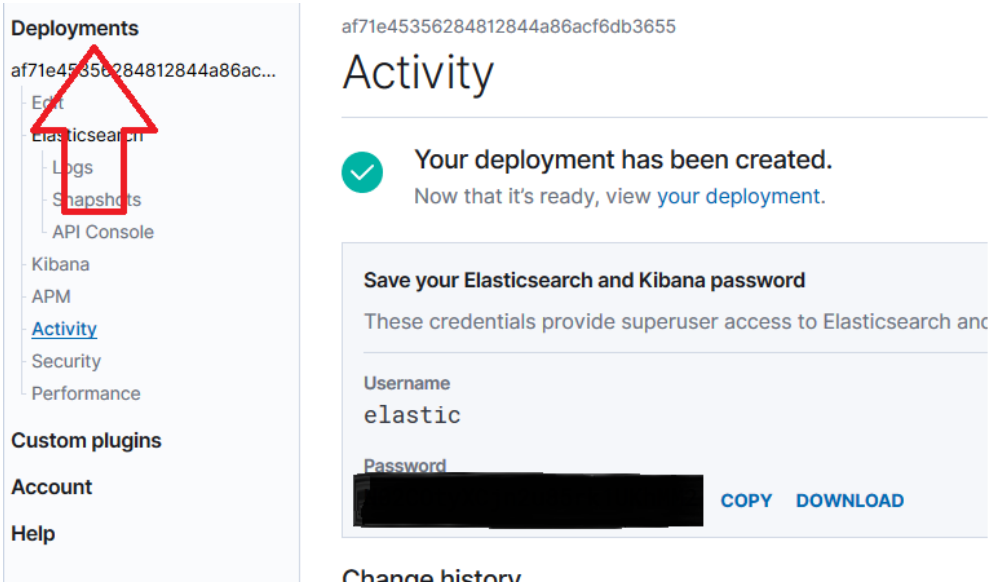


m. Click “Create deployment” located at the bottom of the screen.

n. Save your credentials for the “elastic” user account. You will need this later in the labs. Do not lose this.

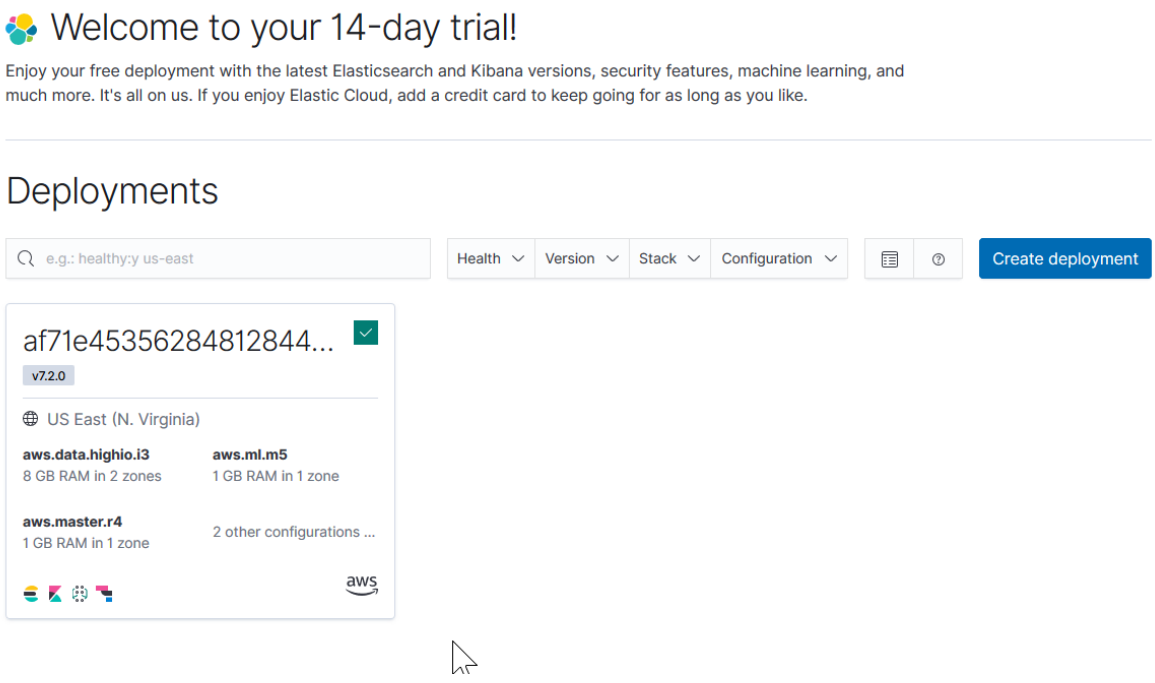


o. Once the deployment is done you should see “Deployments” in the top left corner of your screen. Click “Deployments”



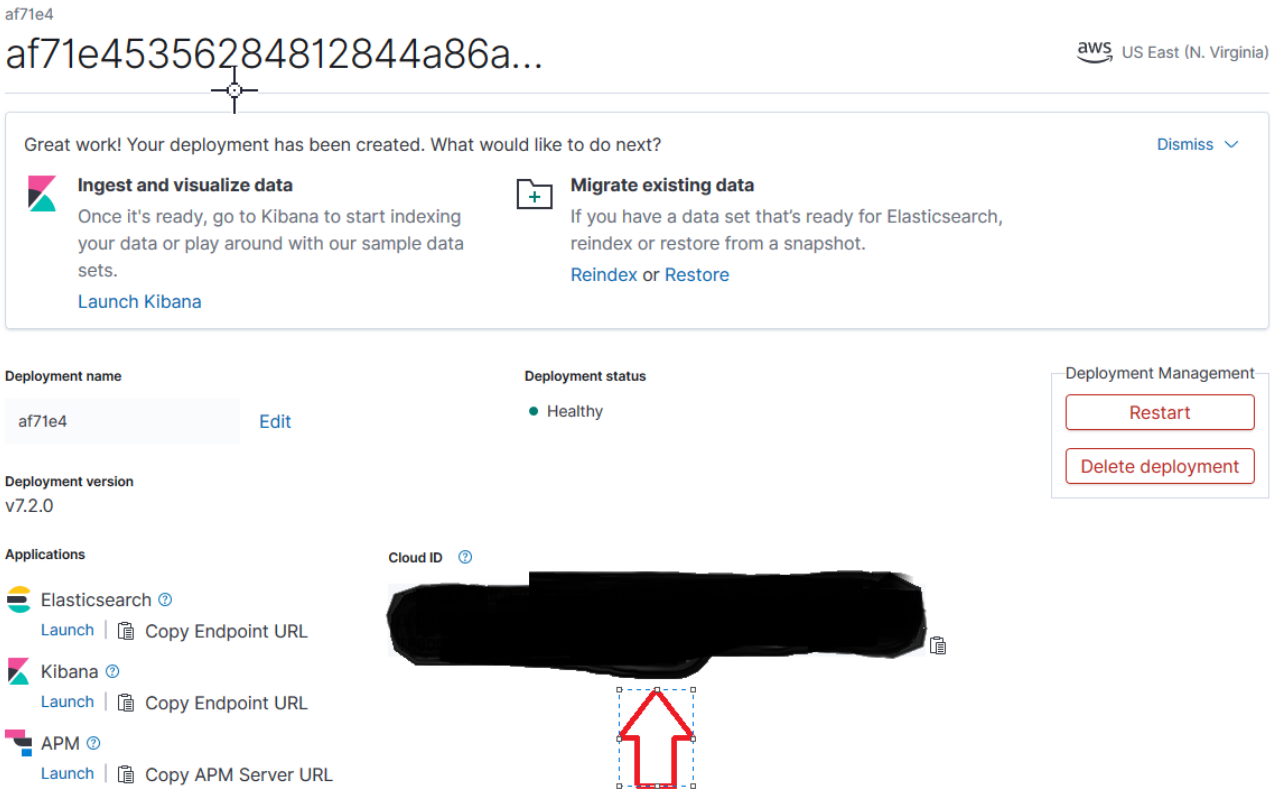
p. You will need the credentials for the “elastic” user later. Copy it to a text editor.

q. You should now see the “Deployments” page and there should be one cluster.

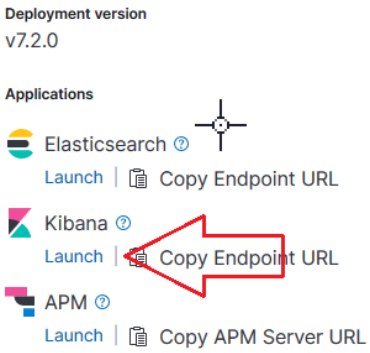


r. Click on the cluster you created.

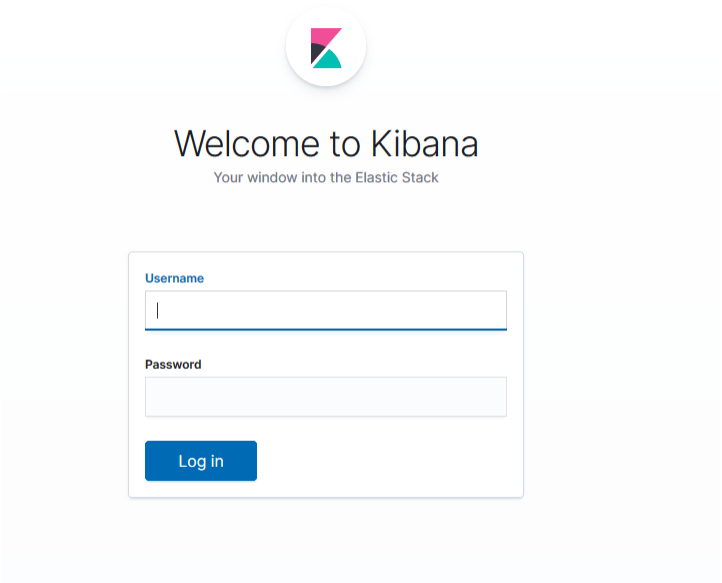
s. You will how see information specific to this cluster. Copy the “Cloud ID” to the same place as you did the “elastic” user in step ‘q’. You will need this later in the lab.



t. Log into your Kibana instance by clicking “Launch” under the Kibana icon:



u. This will start another tab in your browser and put you at the login screen:



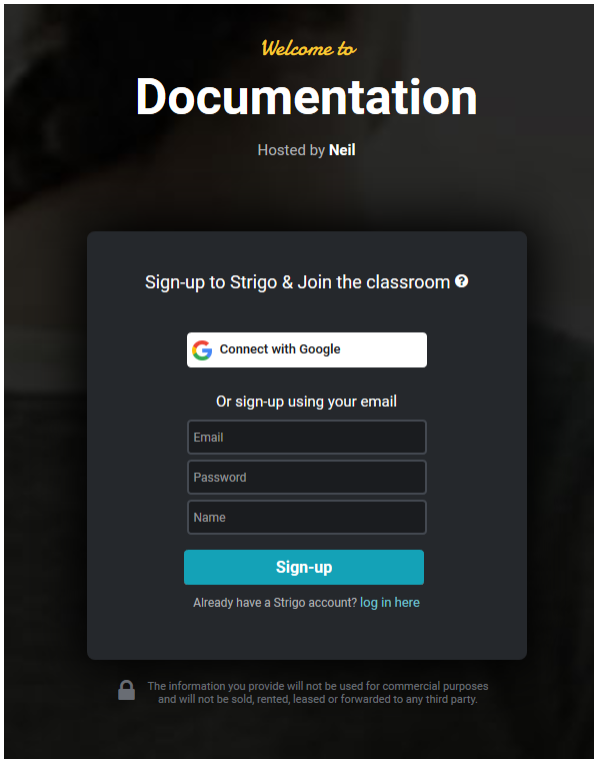
Using your ‘elastic’ userID log into Kibana.

Stop. Do not go into the next lab. If you are managing a SIEM or logging solution today would you have been able to create your infrastructure as quickly as we just did? Feel free to look at the options available to you in your cloud trial. Using the Elastic Cloud provides a way to allow you to focus on the analytics and let us focus on the infrastructure.

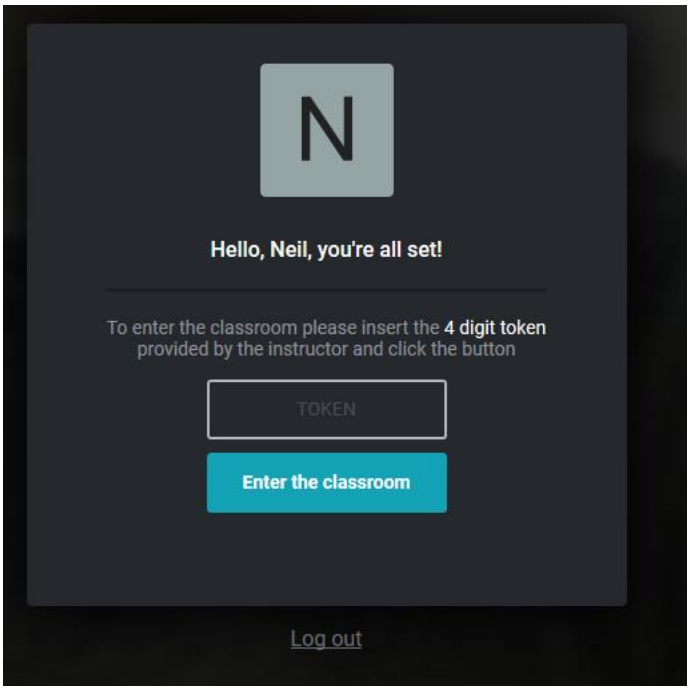
Access your Strigo Environment (Lab 2)

This is where both the Linux and Windows hosts reside.

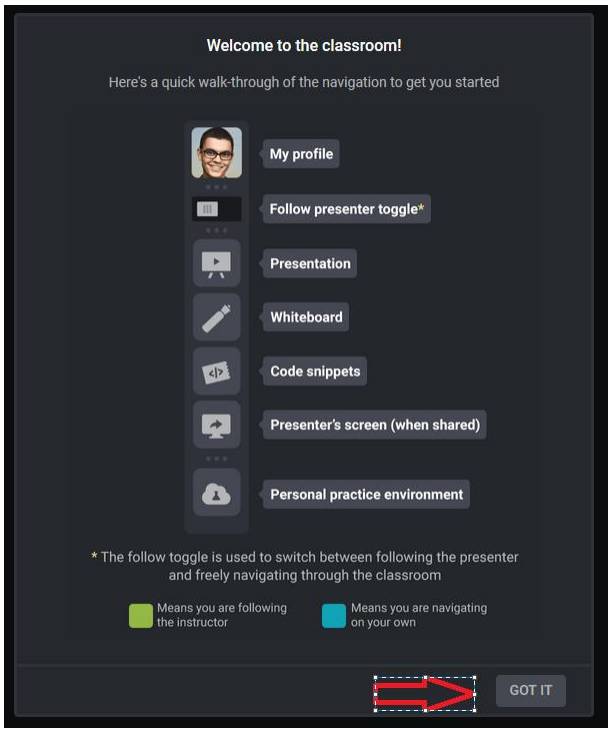
1. Follow the link the instructor provides. You should get to a page that looks like this:



2. Sign up for an account. You will be asked for a token on the next screen. The instructor will provide this for you.

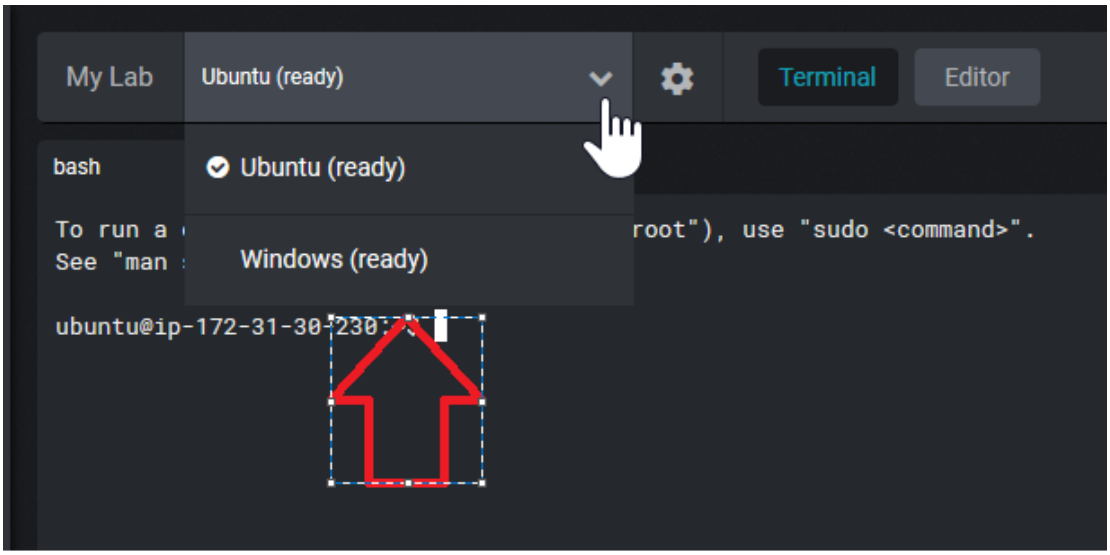


3. Enter the token and click “Enter the Classroom”. Next you will see a screen titled “Welcome to the classroom”. Click “Got it” and the bottom right.



4. Click on the “My Lab” icon on the left.

At the top of the page, next to “My Lab” you will see two hosts available for you to use (Ubuntu and Windows). If you click on the down arrow you will get to choose which host you are interacting with.



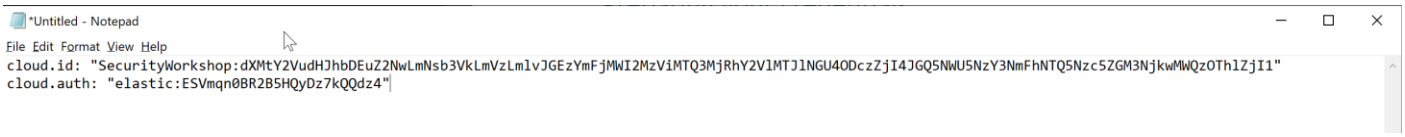
Preparing your credentials

1. From your Elasticsearch Cluster you will need the following:

a. Password for the “elastic” userID
b. CloudID information

2. Using a text editor on your host create a file that has the following contents:

   a. cloud.id: “<INSERT CLOUD ID>”
   b. cloud.auth: “<INSERT ELASTIC ID AND PASSWORD>”



This information will be used in each of the four beats that we install.

Preparing your Ubuntu Host

1. Update the system:

   a. sudo apt-get update

   b. sudo apt-get upgrade
      i. Enter “Y” when asked if you want to install the updates

2. Add the Elastic GPG keys to the package manager.

   a. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add

3. Add the Elastic Debian repository list to the local list of sources:

   a. echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

4. Update the system with the new information:

   a. apt-get update

Installing and Configuring Packetbeat (Lab 3)

1. Install packetbeat:

a. sudo apt-get install packetbeat

2. We need to determine which interface we want packetbeat to listen on. Enter the following command and press ‘enter’ to enumerate all the available devices:

   a. /usr/bin/packetbeat devices

```
ubuntu@ip-172-31-30-230:/etc/packetbeat$ /usr/bin/packetbeat devices
0: eth0 (No description available) (172.31.30.230 fe80::401:64ff:feaf:4538)
1: any (Pseudo-device that captures on all interfaces) (Not assigned ip address)
2: lo (No description available) (127.0.0.1 ::1)
3: nflog (Linux netfilter log (NFLOG) interface) (Not assigned ip address)
4: nfqueue (Linux netfilter queue (NFQUEUE) interface) (Not assigned ip address)
ubuntu@ip-172-31-30-230:/etc/packetbeat$
```

   We want to use ‘eth0’ which is device ‘0’.

3. Edit the ‘/etc/packetbeat/packetbeat.yml’ using the following command:

   a. sudo vi /etc/packetbeat/packetbeat.yml

   b. First, we will configure packetbeat to listen on device ‘0’. Type ‘/’ and enter the text “ any” (note the space before the string ‘any’) and hit enter. Your cursor should be placed at the space before ‘any’.

```
#============================== Network device ================================

# Select the network interface to sniff the data. On Linux, you can use the
# "any" keyword to sniff on all connected interfaces.
packetbeat.interfaces.device: any
```

   c. Type ‘D’. This will erase the text to the end of the line and place the cursor on the colon.

```
#============================== Network device ================================

# Select the network interface to sniff the data. On Linux, you can use the
# "any" keyword to sniff on all connected interfaces.
packetbeat.interfaces.device:
```

d. Type ‘a’ (insert after current cursor placement). Type “ 0” (note the space before ‘0’. Hit the ‘esc’ key to get out of insert mode.

```
#============================== Network device ================================

# Select the network interface to sniff the data. On Linux, you can use the
# "any" keyword to sniff on all connected interfaces.
packetbeat.interfaces.device: 0

#===================================== Flows ======================================
```

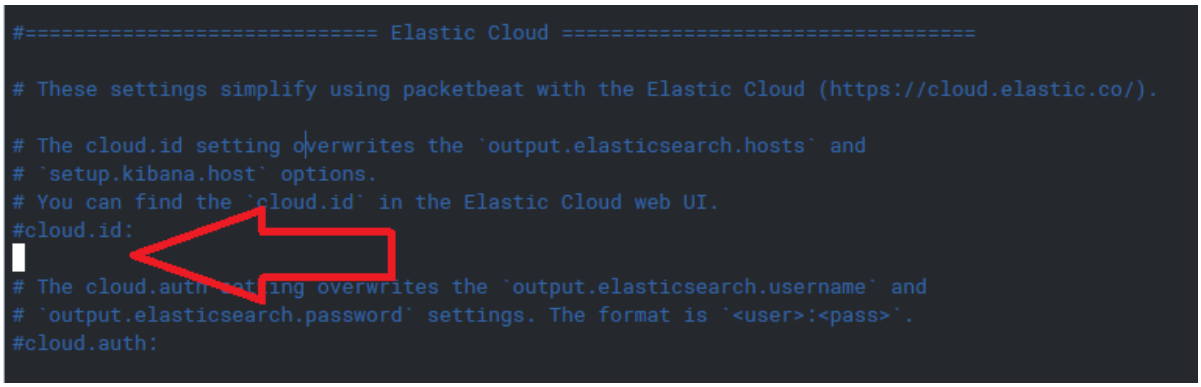
e. Find the part of the config that relates to “Elastic Cloud”. Type ‘/’ (forward slash) and then ‘cloud.id’ like:

```
  - type: redis
    # Configure the ports where to listen for Redis traffic. You can disable
    # the Redis protocol by commenting out the list of ports.
    ports: [6379]
  /cloud.id
```

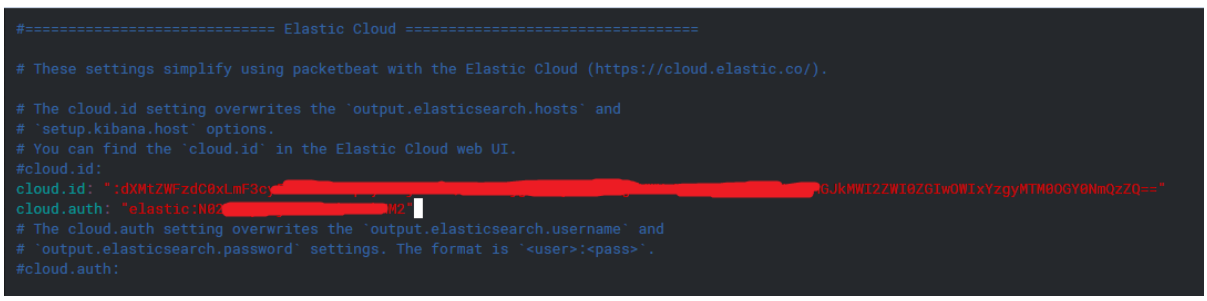
f. Hit “enter” and you should now see that vi found the first instance of the string ‘cloud.id’.

```
#============================ Elastic Cloud ================================

# These settings simplify using packetbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:
```

g. Using the down arrow key navigate to the open line just after “#cloud.id”:



h. To insert the credentials for your cloud instance, go to your text editor and copy the formatted credentials from step 3. Go to your Strigo session. In ‘vi’ type ‘i’. This will put you in ‘insert mode’. Right click and “paste” your credentials.



i. Hit the “escape” key. This will take you out of “insert mode”.

j. Hit “ESC” to get out of “insert mode”. Type “:wq!” (write, quit, now). This will save and close your vi session.

4. Install the Kibana dashboards and search pattern:

   a. sudo packetbeat setup

5. Start packetbeat by typing the following command:

   a. sudo service packetbeat start

Installing and Configuring Auditbeat (Lab 4)

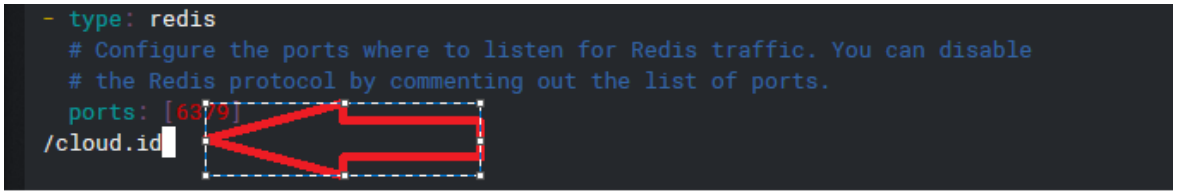
1. Install auditbeat:

    a. sudo apt-get install auditbeat

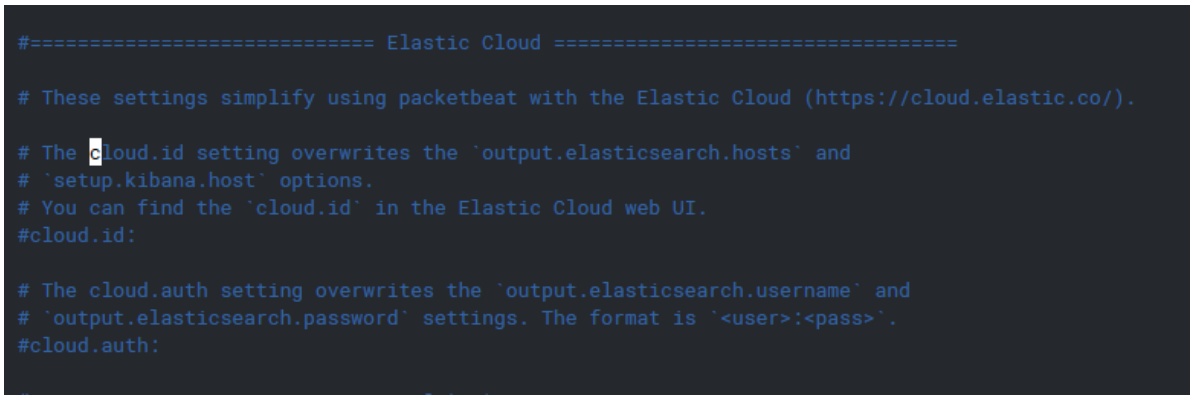
2. Edit the configuration file:

    a. sudo vi /etc/auditbeat/auditbeat.yml

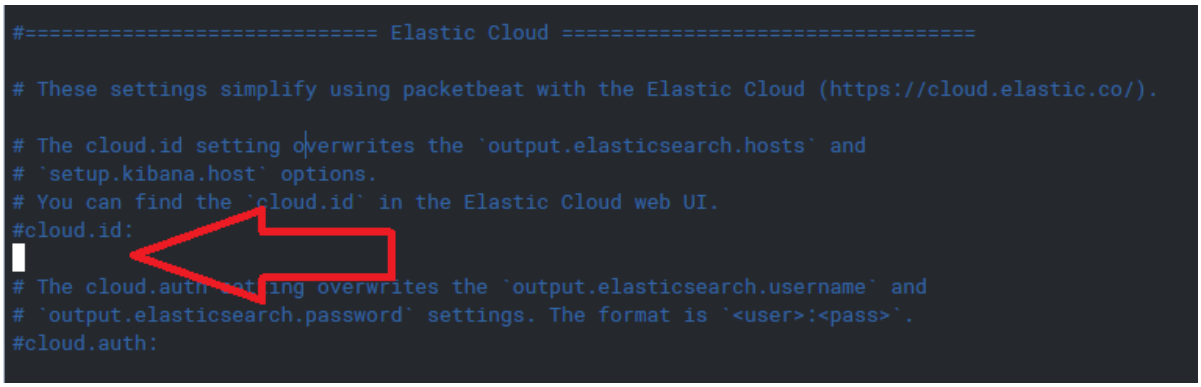
    b. Find the part of the config that relates to “Elastic Cloud”. Type ‘/’ (forward slash) and then ‘cloud.id’ like:



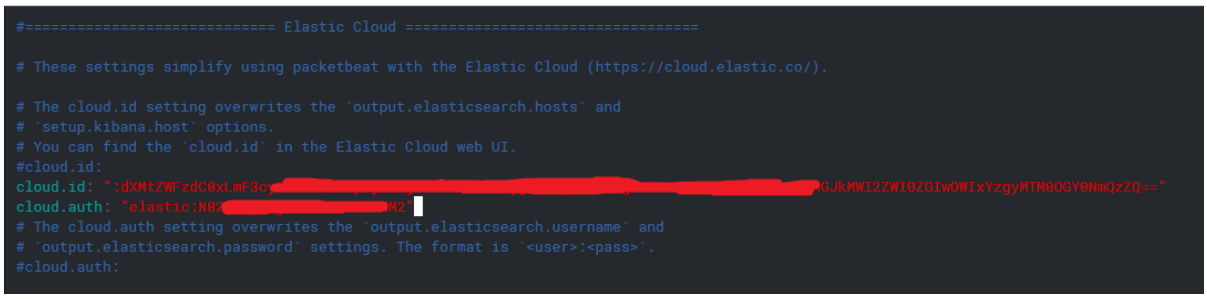
    c. Hit “enter” and you should now see that vi found the first instance of the string ‘cloud.id’.



d. Using the down arrow key navigate to the open line just after “#cloud.id”:



e. To insert the credentials for your cloud instance, go to your text editor and copy the formatted credentials from step 3. Go to your Strigo session. In ‘vi’ type ‘i’. This will put you in ‘insert mode’. Right click and “paste” your credentials.



f. Hit the “escape” key. This will take you out of “insert mode”.

g. Hit “ESC” to get out of “insert mode”. Type “:wq!” (write, quit, now). This will save and close your vi session.

3. Install the dashboards and search patterns:

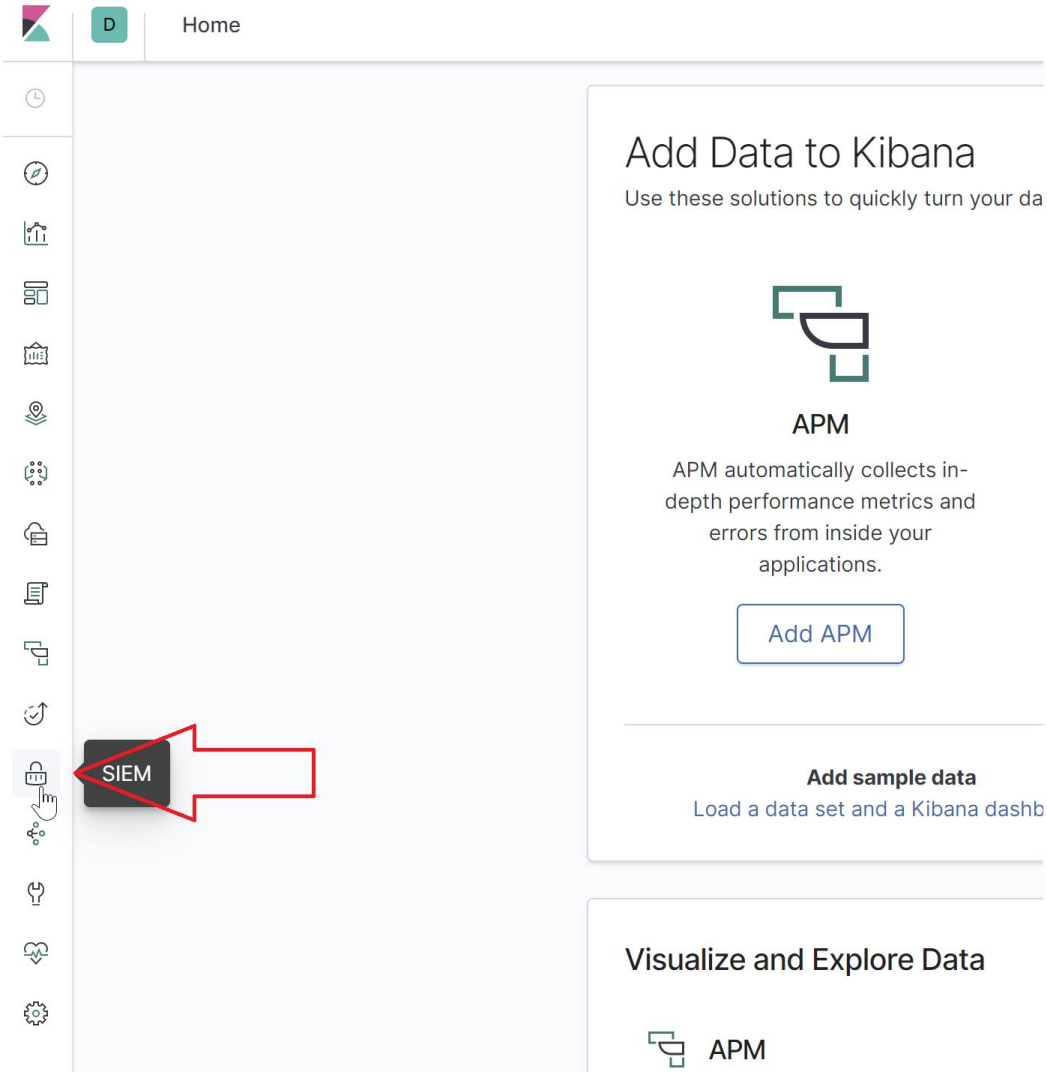
   a. sudo auditbeat setup

4. Start the auditbeat service:

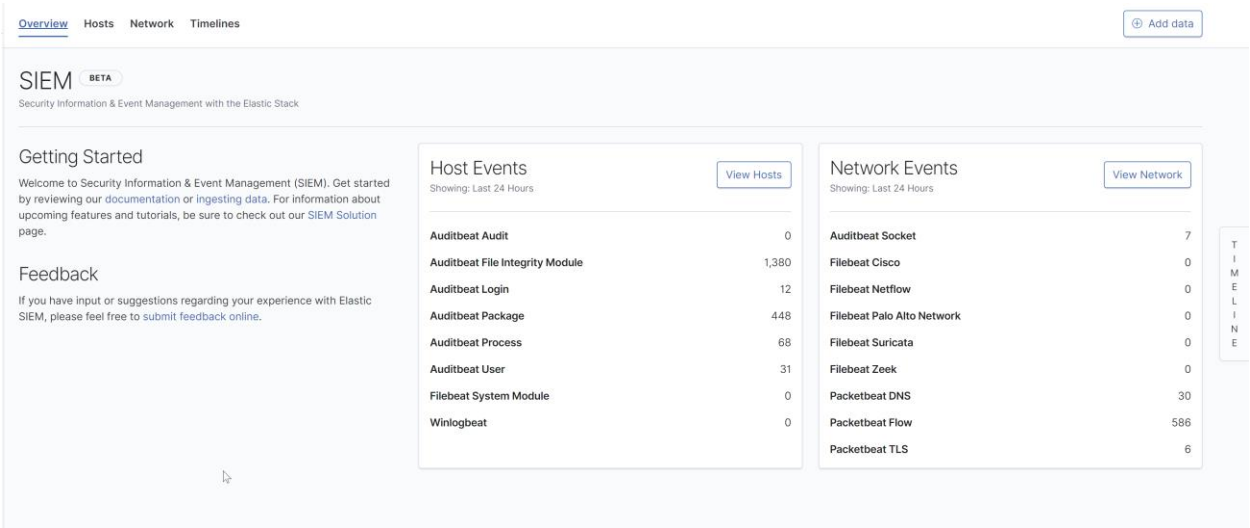
   a. sudo service auditbeat start

View Elastic's SIEM (Lab 5)

1. Go you your Kibana instance and look for a lock icon on the left hand side (5th icon from the bottom):



2. You will see the Overview page will give some high-level information about what type of data we are currently ingesting:



We can see the specific modules that are generating data from a host and network standpoint.

3. At the top of the page are the two current views, host and network, along with the timelines.

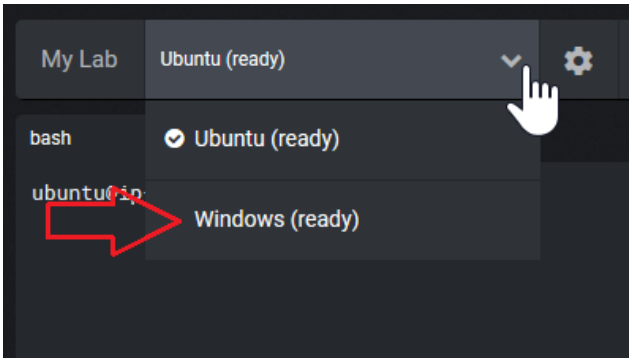
4. Click on Hosts and explore what KPI's are collected and what analytics are being show.

5. Clock on Network and explore what KPI's are collected and what analytics are being show.

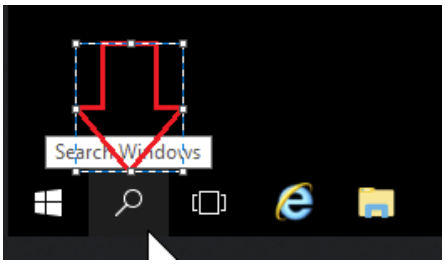
At this point you should have both the host and the network tabs of the SIEM app populated with data. Since you are running on 7.3 you will also notice that there are a few machine learning jobs/recipes that are part of this release. At the top right is "Anomaly Detection". This the SIEM apps hook into Elasticsearch's ML. While there are three jobs that are given away as part of 7.3 you will only notice two of them showing. The jobs shown are based on the index patterns detected. Since we haven't sent Windows logs yet there are no ML jobs for Windows.

Install and Configure Winlogbeat (Lab 6)

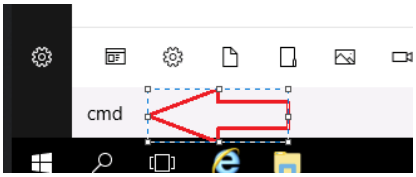
1. In Strigo change to the Windows host by choosing the drop down menu next to “My Lab”.



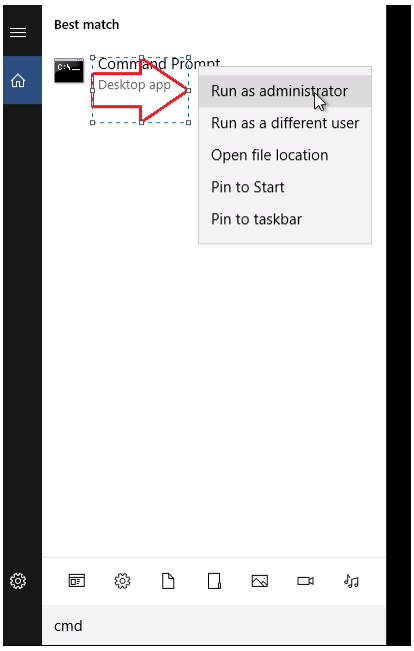
2. Click on the magnifying glass next to the Windows icon in the lower left corner.



3. Type “cmd” and the “Command Prompt” application should appear.



4. Right click on the “Command Prompt” and choose “Run as administrator”.



5. Move to the “C:\” directory and create a new folder called “elastic” and then move into it:

    a. cd \
    b. mkdir elastic
    c. cd elastic

6. A “Command Prompt” should appear. In the command prompt type “powershell” and press enter.

7. Set Powershell to use TLS 1.2 and then download WinLogBeat:

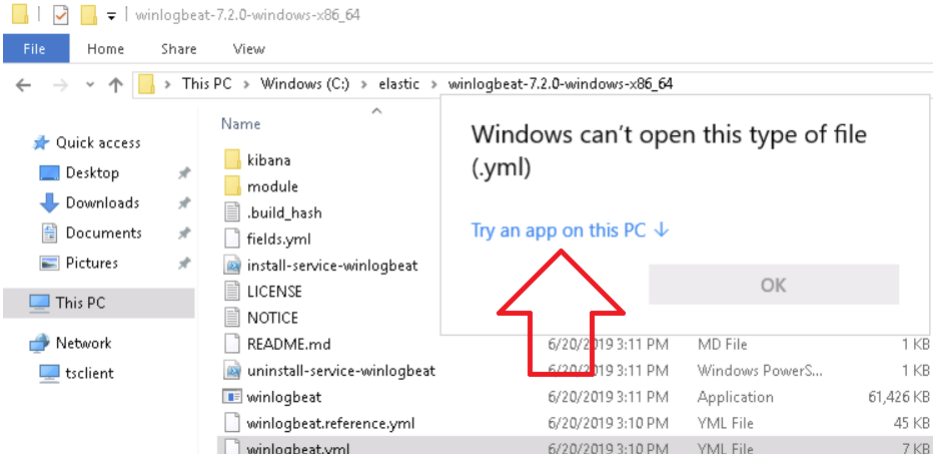
    a. [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
    b. Invoke-WebRequest -URI "https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-7.2.0-windows-x86_64.zip" -Outfile winlogbeat.zip

8. Type the following Powershell command to uncompress the zip file, go into the new directory and install Winlogbeat as a service:

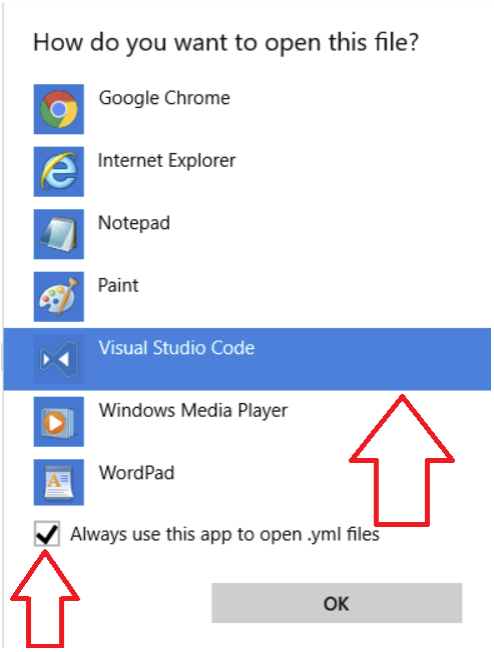
    a. Expand-Archive -path .\winlogbeat.zip -destinationpath .\
    b. cd .\winlogbeat-7.2.0-windows-x86_64\

c. .\install-service-winlogbeat.ps1

9. In Windows Explorer navigate to the “winlogbeat-7.2.0-windows-x86_64” directory and double-click in the “winlogbeat.yml” file. You will get a message that “Windows can’t open this type of file (.yml)”. Click on “Try an app on this PC”.



10. You will get a new screen “How do you want to open this file?” Check the box for “Always use this app to open .yml files.” Click on “Visual Studio Code”.



11. Copy/paste your credentials (cloud.id and cloud.auth) into the configuration file in the "Elastic Cloud" section.

```
#============================ Elastic Cloud ================================

# These settings simplify using winlogbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:
cloud.id: ":dXMtZWFzdCOxLmk[redacted]2ZWIOZGIwOWIxYzgyMTMOOGYONmQzZQ=="
cloud.auth: "elastic:NO[redacted]"

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:
```

12. Setup dashboards:

    a. .\winlogbeat.exe setup –dashboards

13. Start the Winlogbeat service by typing:

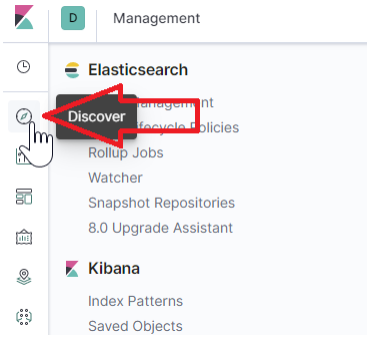
    a. Start-Service Winlogbeat

```
PS C:\Users\Administrator\Downloads\winlogbeat-7.2.0-windows-x86_64> Start-Service Winlogbeat
PS C:\Users\Administrator\Downloads\winlogbeat-7.2.0-windows-x86_64>
```

Viewing Windows Dashboards and Data (Lab 7)

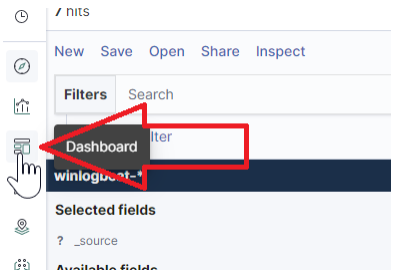
1. Go to your Kibana instance.

2. Go to the Discover tab.

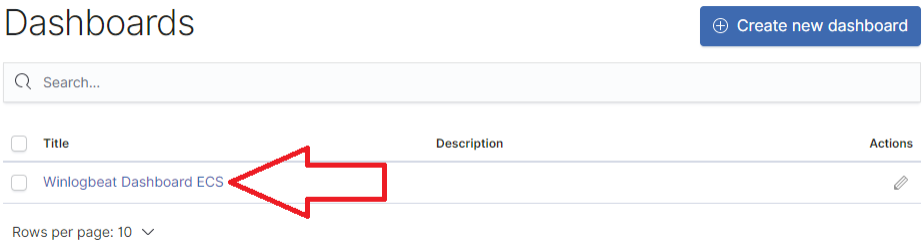


3. Look at the hits counter and the histogram. Notice that the default policy on this Windows hosts doesn't have much logging enabled.

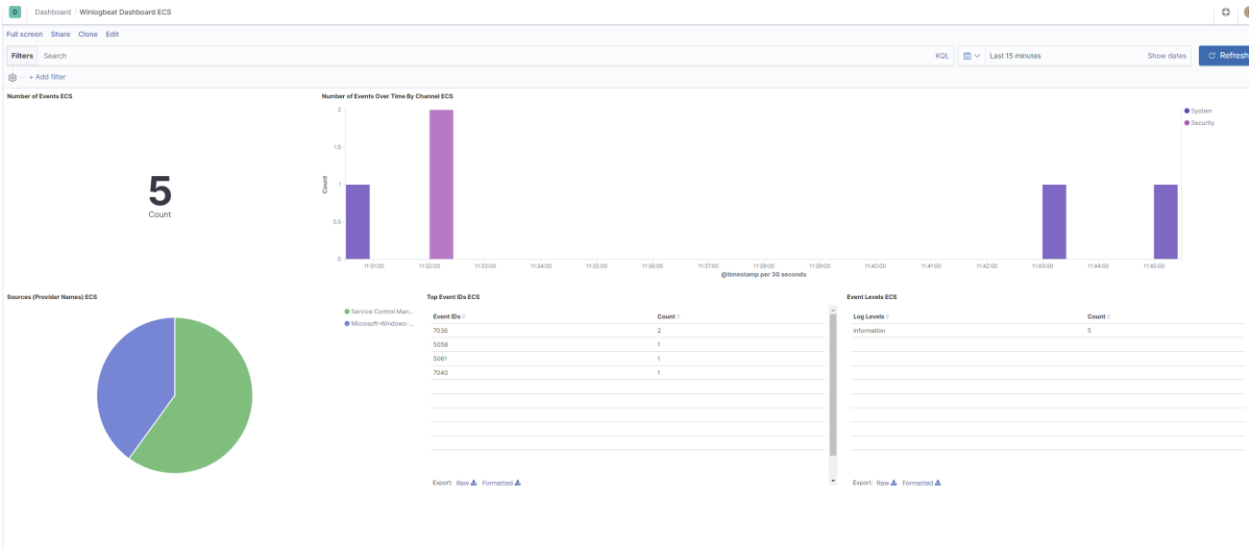
4. Look at the dashboard that is included in the module for WinLogBeat. Click on "Dashboards"



5. Click on “Winlogbeat Dashboard ECS”



6. While we have a few visualizations, they are limited in what they are showing because we don’t have enough events.



When you look at your data do you know why you get the results you do? Part of being able to do good analysis is to have knowledge about what should be sent and knowledge of the type of data that is expected. Just because there is data, doesn’t mean it’s the right data or all the data. As analysts we need to be more rigorous in our approach to security analytics/threat hunting. Understanding your data and ensuring it’s quality will allow you to have a higher expectation of correct results.

Editing the Windows Audit Policy (Lab 8)

1. In the “Powershell Prompt” type “auditpol /get /category:*”. This will show the current audit policy settings. This is a detailed view and gives more information that the basic view.

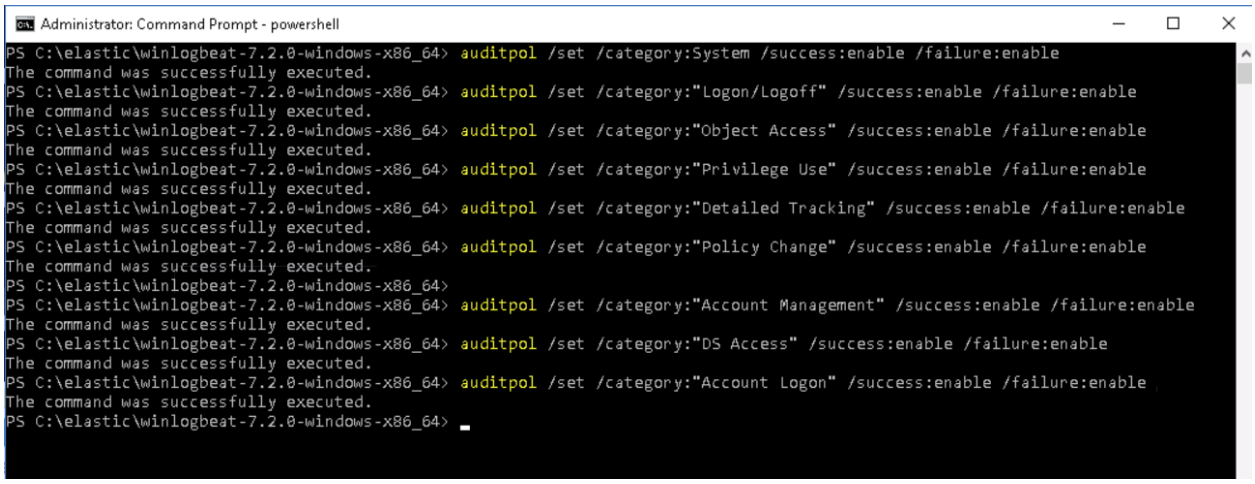
    a. auditpol /get /category:*

```
Administrator: Command Prompt - powershell
PS C:\elastic\winlogbeat-7.2.0-windows-x86_64> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     Success
  Authentication Policy Change            Success
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             Success
  Security Group Management               Success
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 Success
DS Access
  Directory Service Access                Success
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         Success
  Credential Validation                   Success
PS C:\elastic\winlogbeat-7.2.0-windows-x86_64>
```

    Notice how many of the audit settings are set to “No Auditing”.

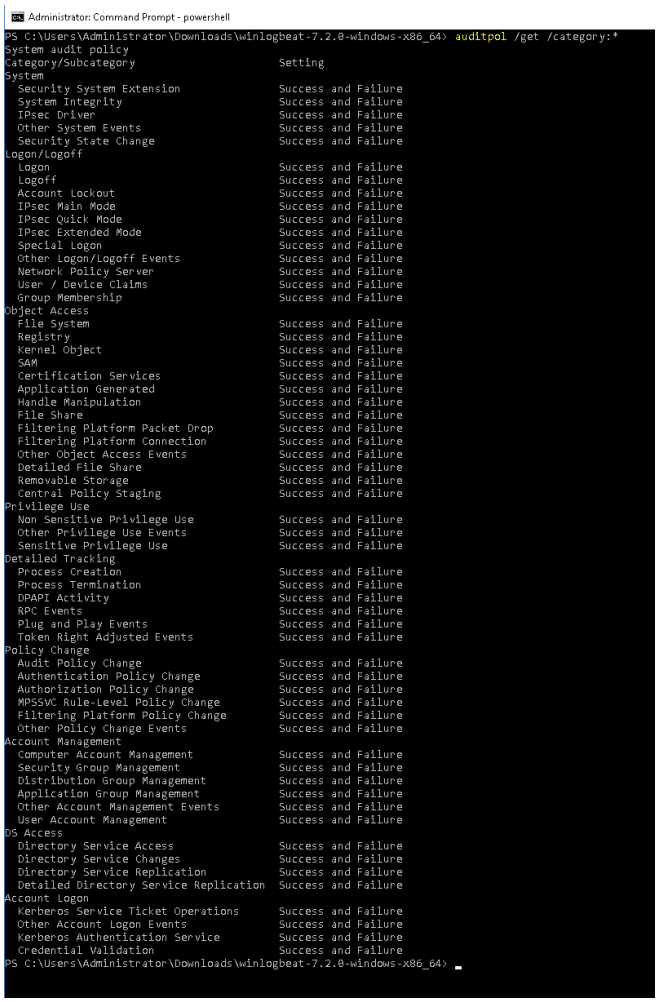
2. Using the following commands, we will enable all of the audit settings to log “Success” and “Failure”

a. auditpol /set /category:System /success:enable /failure:enable
b. auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
c. auditpol /set /category:"Object Access" /success:enable /failure:enable
d. auditpol /set /category:"Privilege Use" /success:enable /failure:enable
e. auditpol /set /category:"Detailed Tracking" /success:enable /failure:enable
f. auditpol /set /category:"Policy Change" /success:enable /failure:enable
g. auditpol /set /category:"Account Management" /success:enable /failure:enable
h. auditpol /set /category:"DS Access" /success:enable /failure:enable
i. auditpol /set /category:"Account Logon" /success:enable /failure:enable



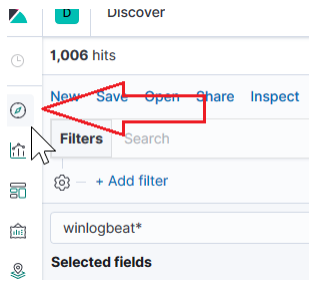
3. Check the status of the the log settings after we enabled everything

   a. auditpol /get /category:*

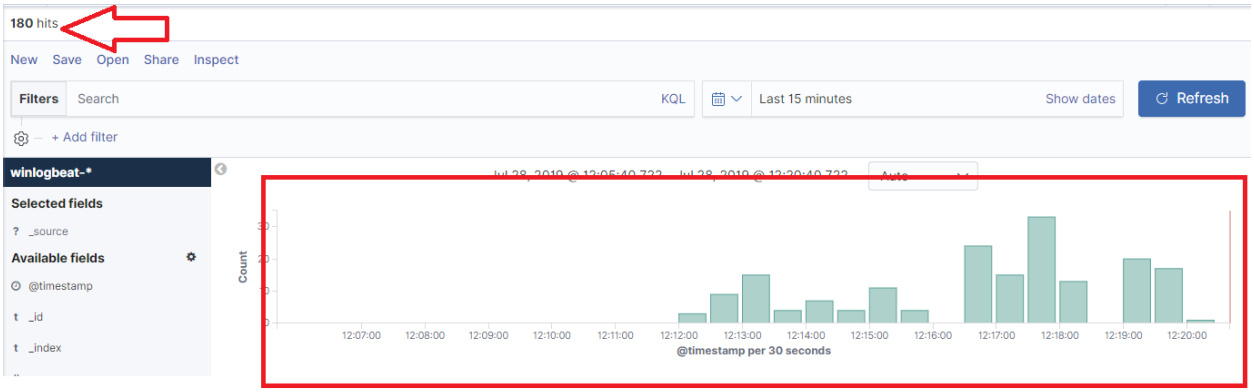


```
Administrator: Command Prompt - powershell
PS C:\Users\Administrator\Downloads\winlogbeat-7.2.0-windows-x86_64> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
  Group Membership                        Success and Failure
Object Access
  File System                             Success and Failure
  Registry                                Success and Failure
  Kernel Object                           Success and Failure
  SAM                                     Success and Failure
  Certification Services                  Success and Failure
  Application Generated                   Success and Failure
  Handle Manipulation                     Success and Failure
  File Share                              Success and Failure
  Filtering Platform Packet Drop          Success and Failure
  Filtering Platform Connection           Success and Failure
  Other Object Access Events              Success and Failure
  Detailed File Share                     Success and Failure
  Removable Storage                       Success and Failure
  Central Policy Staging                  Success and Failure
Privilege Use
  Non Sensitive Privilege Use             Success and Failure
  Other Privilege Use Events              Success and Failure
  Sensitive Privilege Use                 Success and Failure
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Success and Failure
  DPAPI Activity                          Success and Failure
  RPC Events                              Success and Failure
  Plug and Play Events                    Success and Failure
  Token Right Adjusted Events             Success and Failure
Policy Change
  Audit Policy Change                     Success and Failure
  Authentication Policy Change            Success and Failure
  Authorization Policy Change             Success and Failure
  MPSSVC Rule-Level Policy Change         Success and Failure
  Filtering Platform Policy Change        Success and Failure
  Other Policy Change Events              Success and Failure
Account Management
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
DS Access
  Directory Service Access                Success and Failure
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\Users\Administrator\Downloads\winlogbeat-7.2.0-windows-x86_64>
```

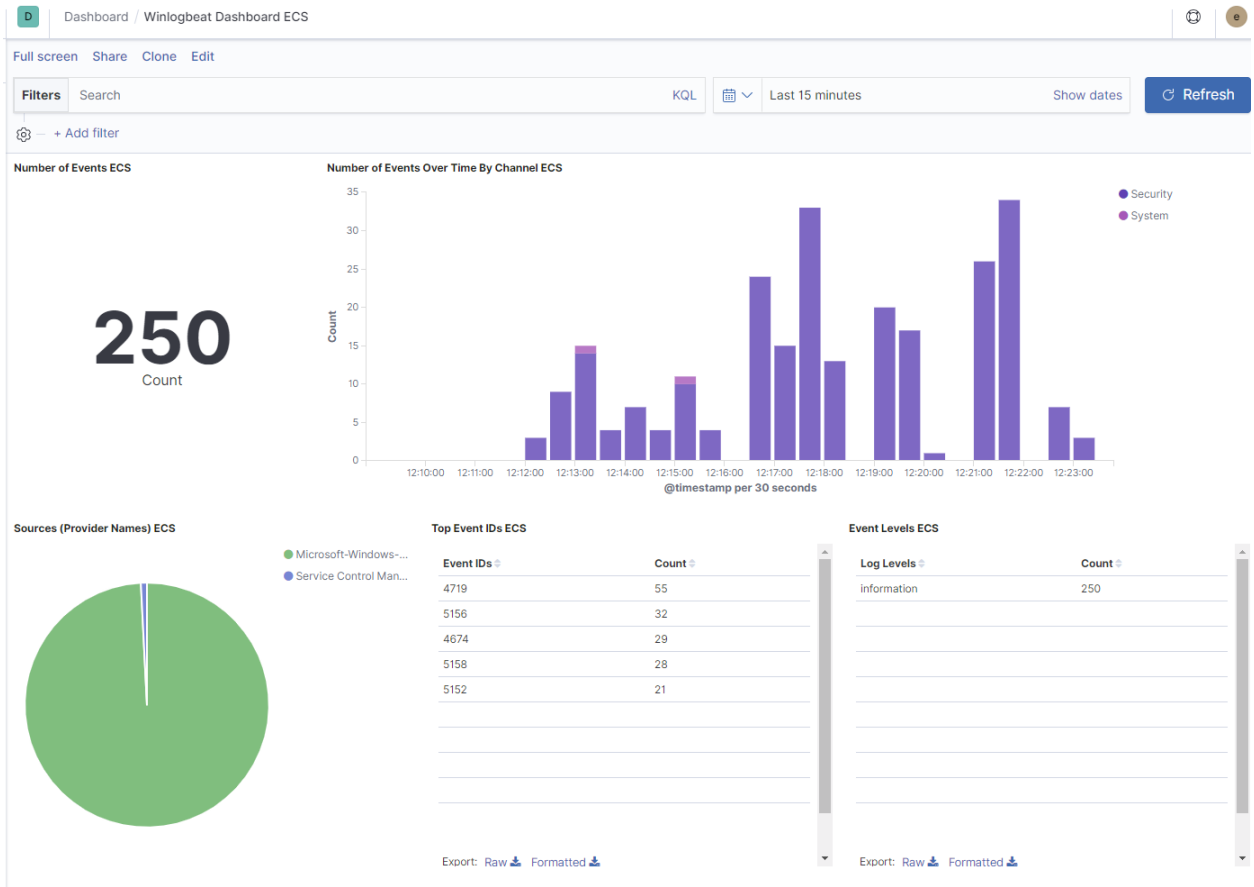
4. Using Kibana's Discover see the events that are coming in.



5. There should be more events coming in now that everything is enabled.



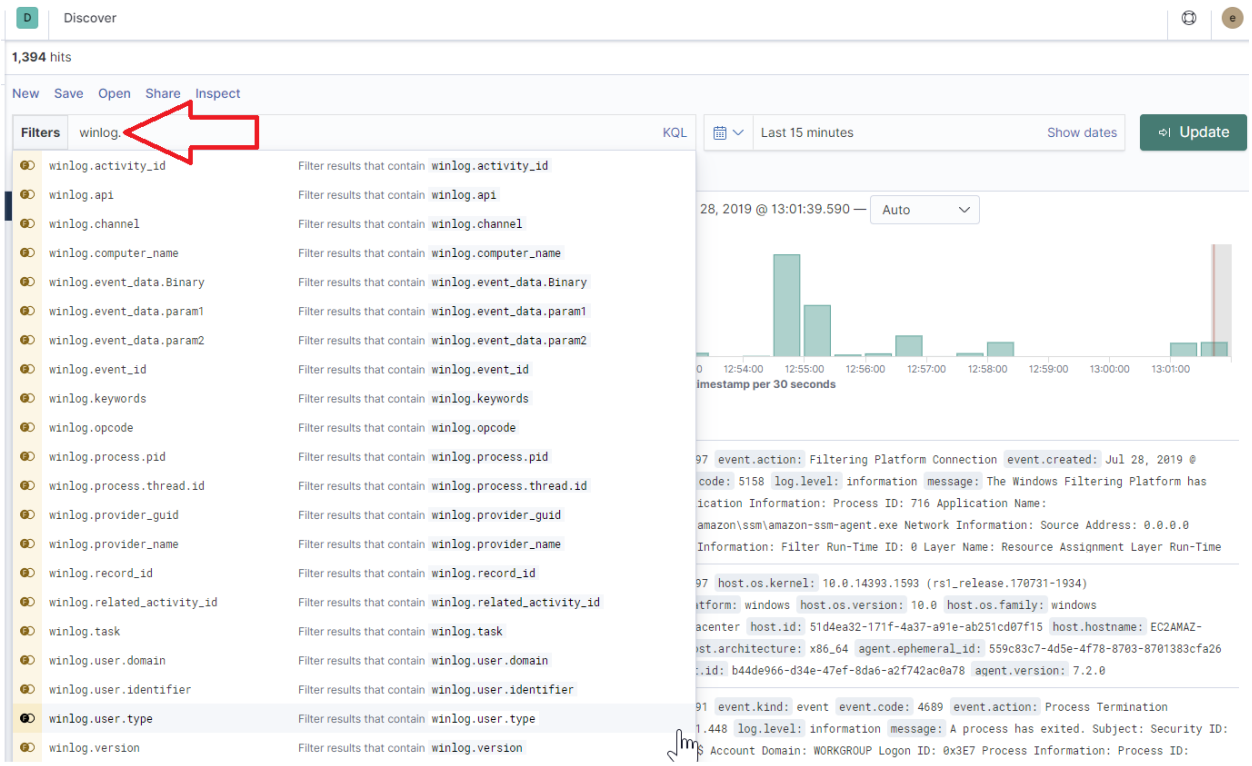
6. Check the "Winlogbeat Dashboard ECS" and see how it looks now.



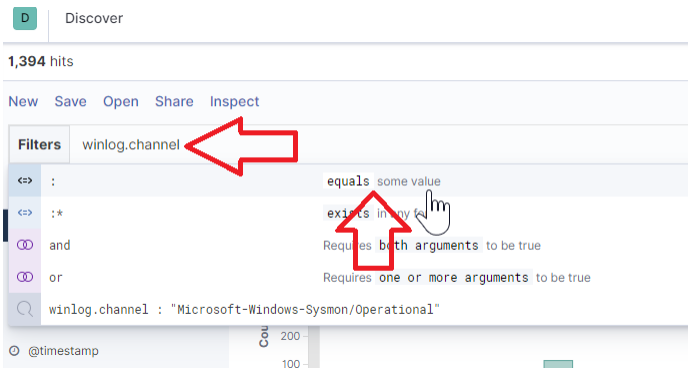
Installing and Configuring Sysmon (Lab 9)

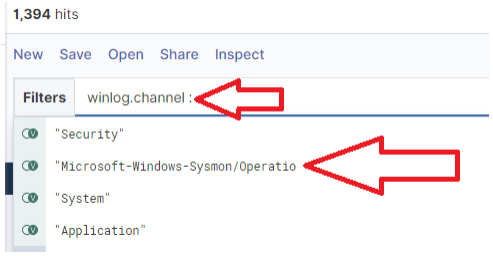
1. In the Powershell prompt change to the “C:\elastic” directory:
    a. cd c:\elastic
2. Using Powershell download sysmon:
    a. Invoke-WebRequest -URI "https://download.sysinternals.com/files/Sysmon.zip" -Outfile sysmon.zip
3. Unzip the sysmon.zip file. Using the Powershell Console type:
    a. Expand-Archive -Path .\Sysmon.zip -DestinationPath .\
4. Install Sysmon, using the XML file for configuration by typing:
    a. .\sysmon.exe -accepteula -i -h md5 -n -l
5. Restart the Winlogbeat service:
    a. Restart-Service Winlogbeat

6. Verify that Sysmon events are being ingested by going to the Kibana Discover tab. In the KQL filters area start to type “winlog.” Notice that Kibana’s KQL Auto Complete feature is helping guide the search by showing all the fields that start with the string “winlog.” You can either continue typing and KQL Auto Complete will continue to filter the results based on what you type of you can select from one of the shown fields.

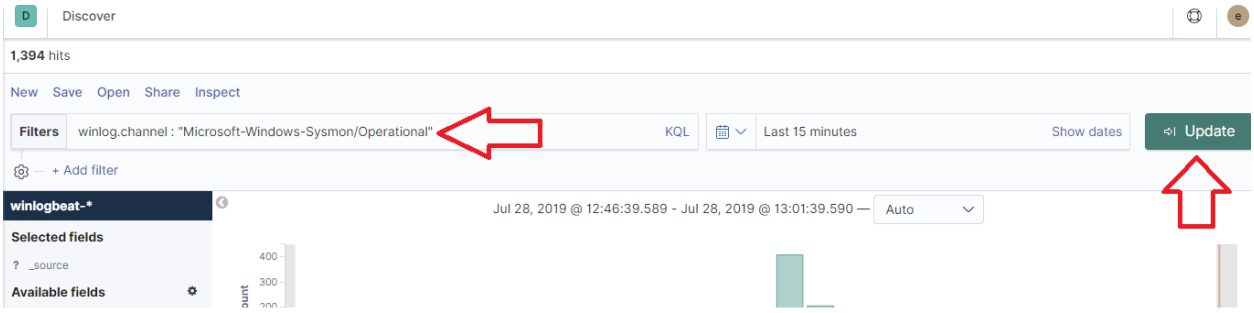


Continue typing, or select, “winlog.channel”. You will notice that KQL will then suggest operators for you to choose how you want to filter based on that field. Choose the “equals some value” option and KQL will suggest possible values that can be searched for.

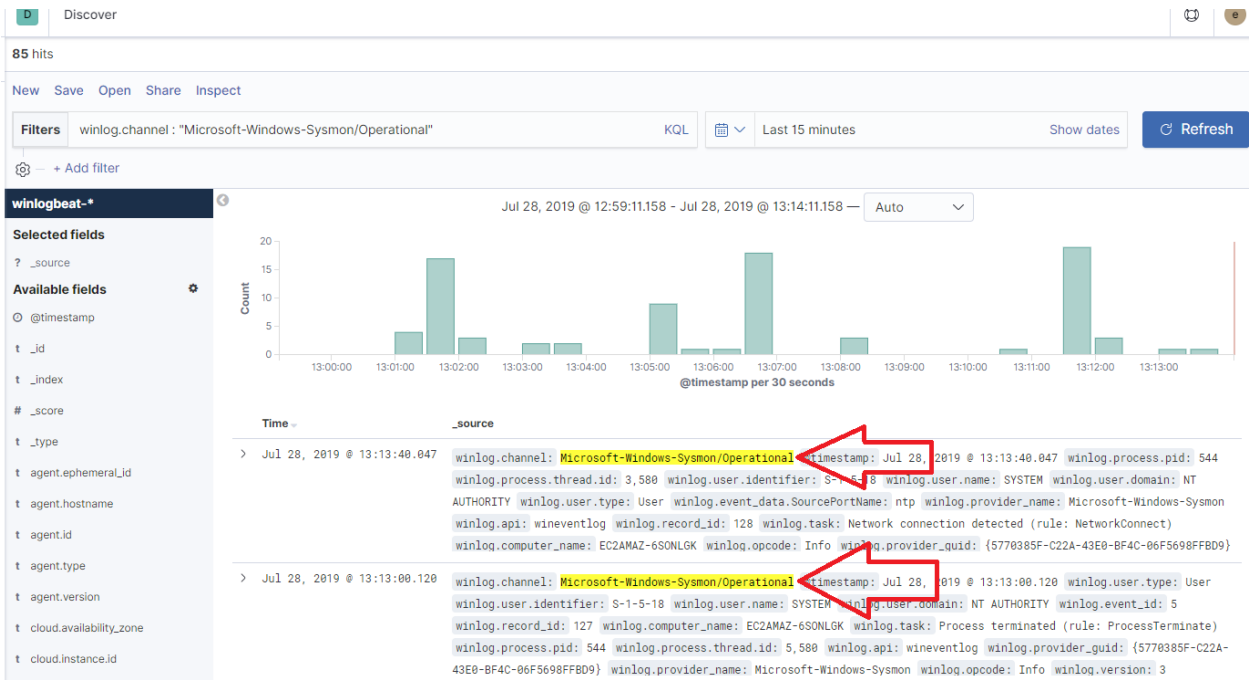




Choose “Microsoft-Windows-Sysmon/Operational” and click “Update”:



You should now only see events from Sysmon. You can verify this by looking at the text highlighted in yellow. This is showing what the filter matched on.



Viewing All Available Windows Log Sources (Lab 10)

1. In the “Powershell Prompt” type:

    a. To get a list of all the Windows Logs that are in the Windows Event Log format:

        i. Get-WinEvent -Listlog *

```
PS C:\elastic> Get-WinEvent -ListLog * | more

LogMode   MaximumSizeInBytes RecordCount LogName
-------   ------------------ ----------- -------
Circular            20971520         115 Application
Circular            20971520           0 HardwareEvents
Circular             1052672           0 Internet Explorer
Circular            20971520           0 Key Management Service
Circular            20971520        2875 Security
Circular            20971520         712 System
Circular            15728640         346 Windows PowerShell
Circular            20971520             ForwardedEvents
Circular            10485760           0 Microsoft-AppV-Client/Admin
Circular            10485760           0 Microsoft-AppV-Client/Operational
```

Windows Logging, unlike *NIX logs, doesn't keep a history of log files, by default. It treats the logs files as a circular buffer. The two settings that effect what happen when the buffer is full is the LogMode and MaximumSizeInBytes. The LogMode will determine what happens when the log gets full. There are thee possible options: AutoBackup, Circular, Retain. The option that is best is Circular. This will overwrite older events, as needed. The RecondCount tells you how many events are in that specific log.

b. To get just the name of the Windows Logs:

    i. Get-WinEvent -ListLog * | Select-Object LogName

c. To see how many logs are available:

    i. Get-WinEvent -ListLog * | Select-Object LogName | Measure-Object | Select-Object Count

d. To find the naming convention for the Sysmon Log:

    i. Get-WinEvent -Listlog * | Select-Object LogName | Select-String -Pattern "Sysmon"

e. The value of "LogName" is what is used in the winlogbeat.yml file for the source name. Look at your winlogbeat.yml file and verify this.

The objective of this lab is to understand what logs are available and make an informed decision on which logs you want to collect. You can see there are a significant amount of logs to choose from.

Install Packetbeat on Windows (Lab 11)

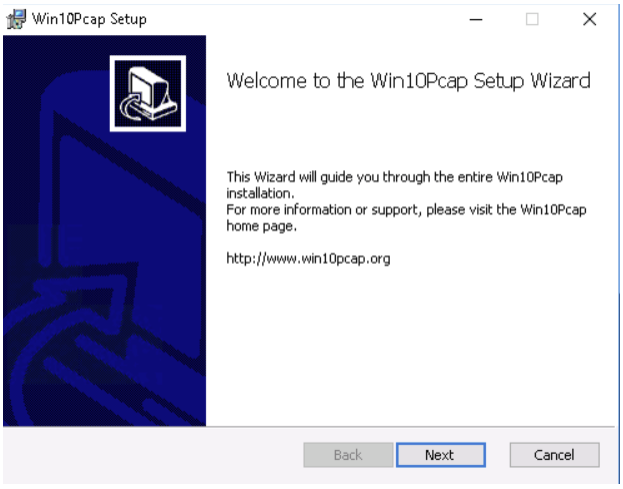
1. Use Powershell to download the following file:

    a. Invoke-WebRequest -URI "https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.2.0-windows-x86_64.zip" -Outfile packetbeat.zip

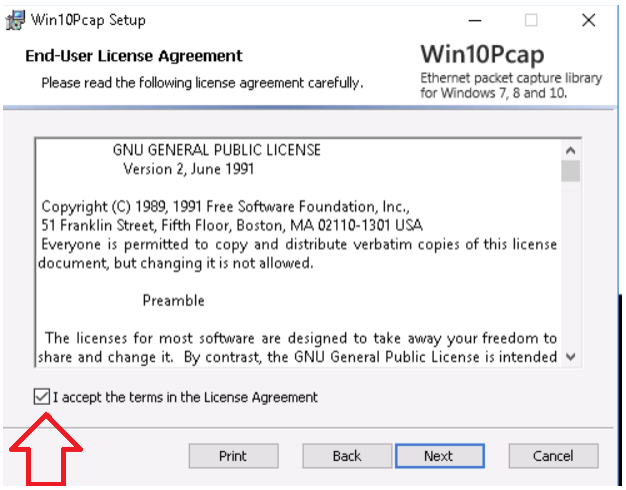
2. Use Powershell to download the following file:

    a. Invoke-WebRequest -URI "http://www.win10pcap.org/download/Win10Pcap-v10.2-5002.msi" -Outfile winpcap.msi

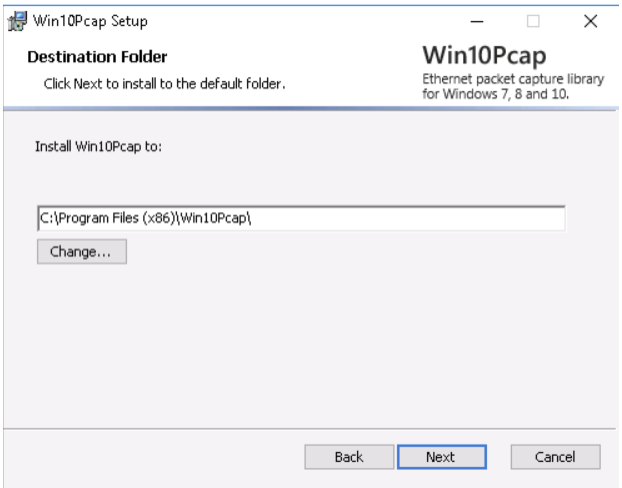
3. Using “Windows Explorer” navigate to the folder “C:\elastic” and double-click on the winpcap.exe” file and click “Next”.



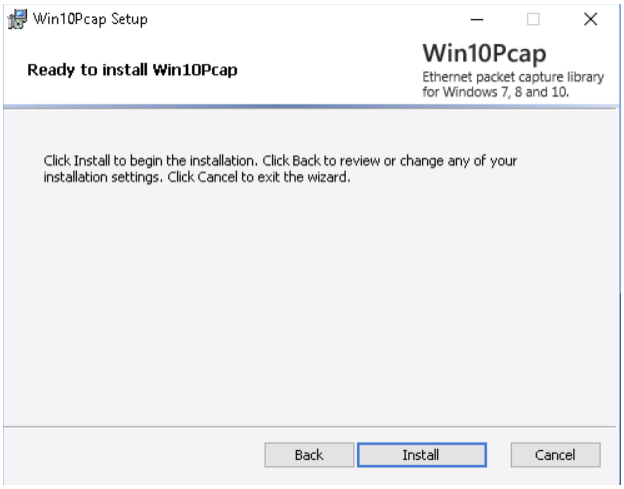
4. Check the box for “I accept the terms in the License Agreement” and click “Next”.



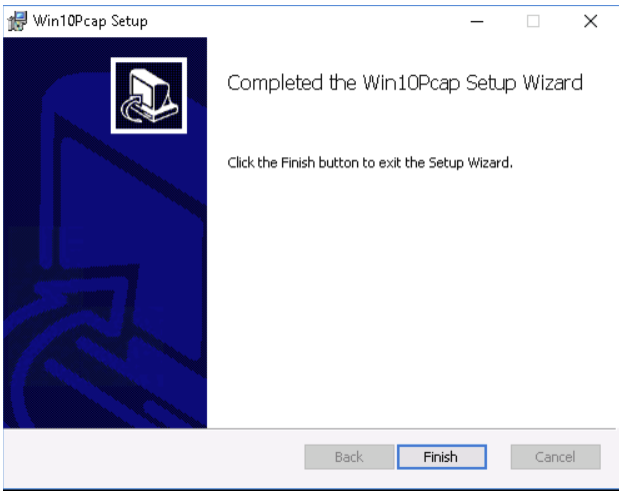
5. Keep the default destination folder and click “Next”.



6. Click “Install”



7. Click “Finish”



8. Unzip the packetbeat.zip file using the following command:

    a. Expand-Archive -Path .\packetbeat.zip -Destination .

9. In the “Powershell Promt” navigate to:

    a. C:\elastic\packetbeat-7.2.0-windows-x86_64

10. Enumerate the available network interfaces available for packet capture using the following command:

    a. .\ packetbeat.exe devices

```
C:\Users\Administrator\Downloads\packetbeat\packetbeat-7.2.0-windows-x86_64>.\packetbeat devices
0: {419F25B1-40DF-49AD-B36D-2C5601117C45} (Citrix) (172.31.28.153)
```

11. Using Visual Studioto edit the packetbeat.yml file to change the following:

    a. Add your Cloud.auth and Cloud.id information

    b. Save the file.

12. Install the Packetbeat services using the following command:

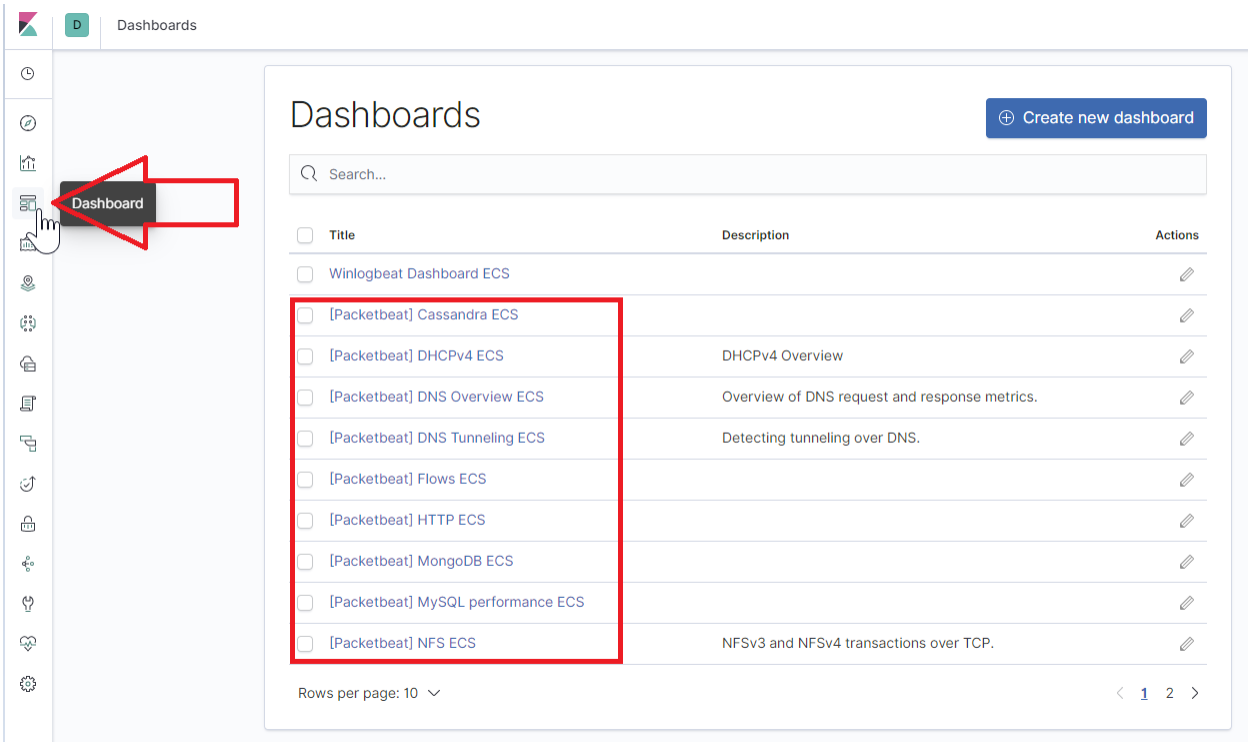
    a. .\install-service-packetbeat.ps1

13. Start the Packetbeat service by typing:

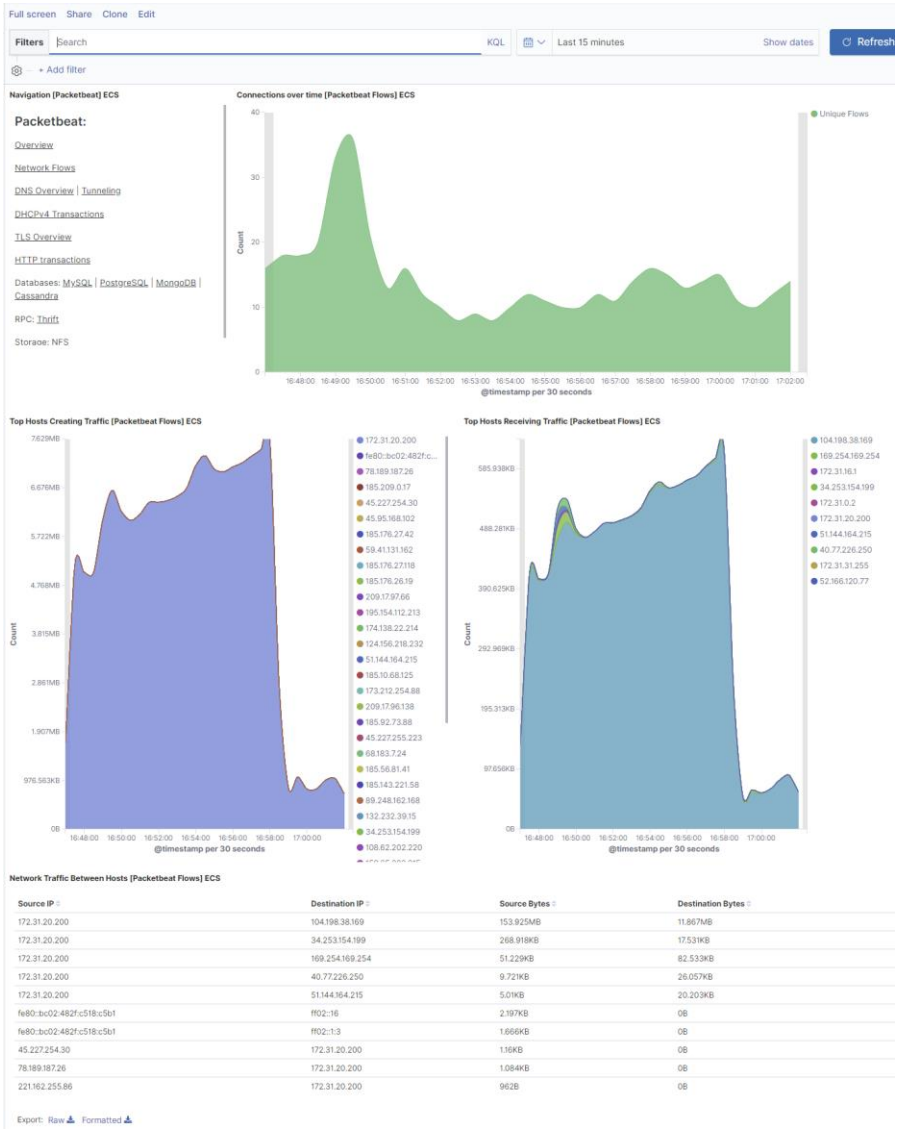
    a. Start-Service Packetbeat

Viewing Packetbeat Data (Lab 12)

1. Go to your Kibana dashboards and see the default dashboards that are part of the packetbeat module.



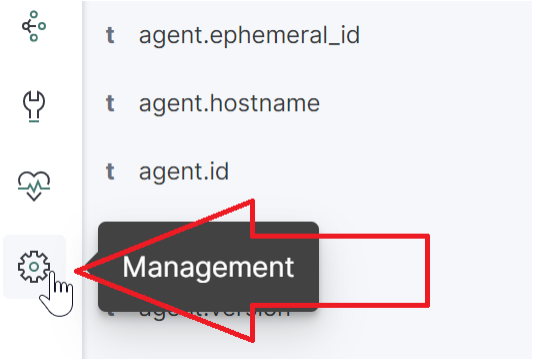
2. Click on the “[Packetbeat] Flows ECS” dashboard.



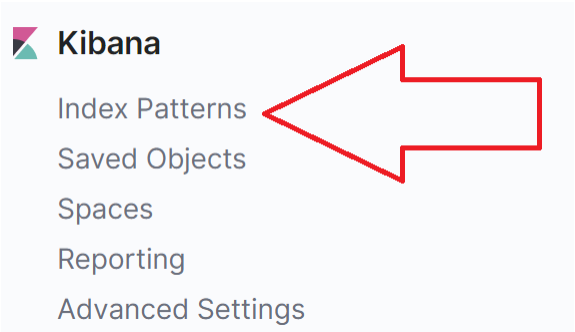
Implicit Correlations and the Power of ECS (Lab 13)

1. Create a new search pattern that will allow us to search both packetbeat and winlogbeat data:

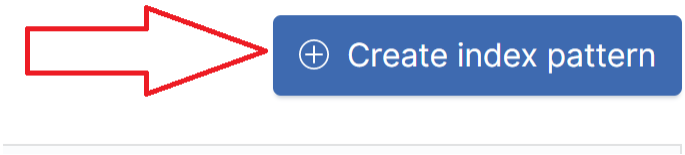
    a. Got to Kibana Management (bottom icon on the left)



2. Click on “Index Patterns”

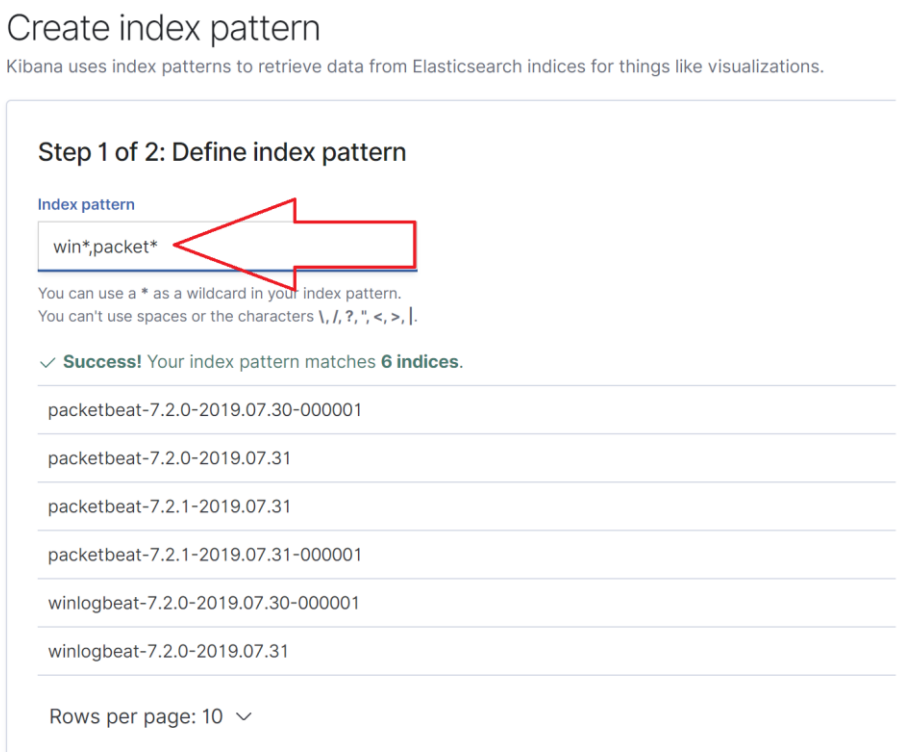


3. Click on “Create Index Pattern”

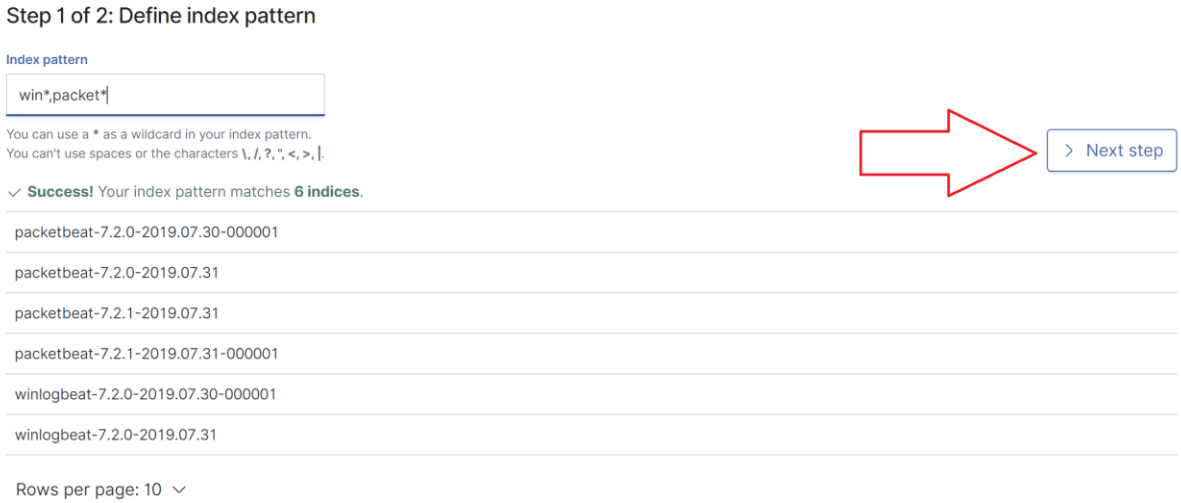


4. In the “Index Pattern” box type:

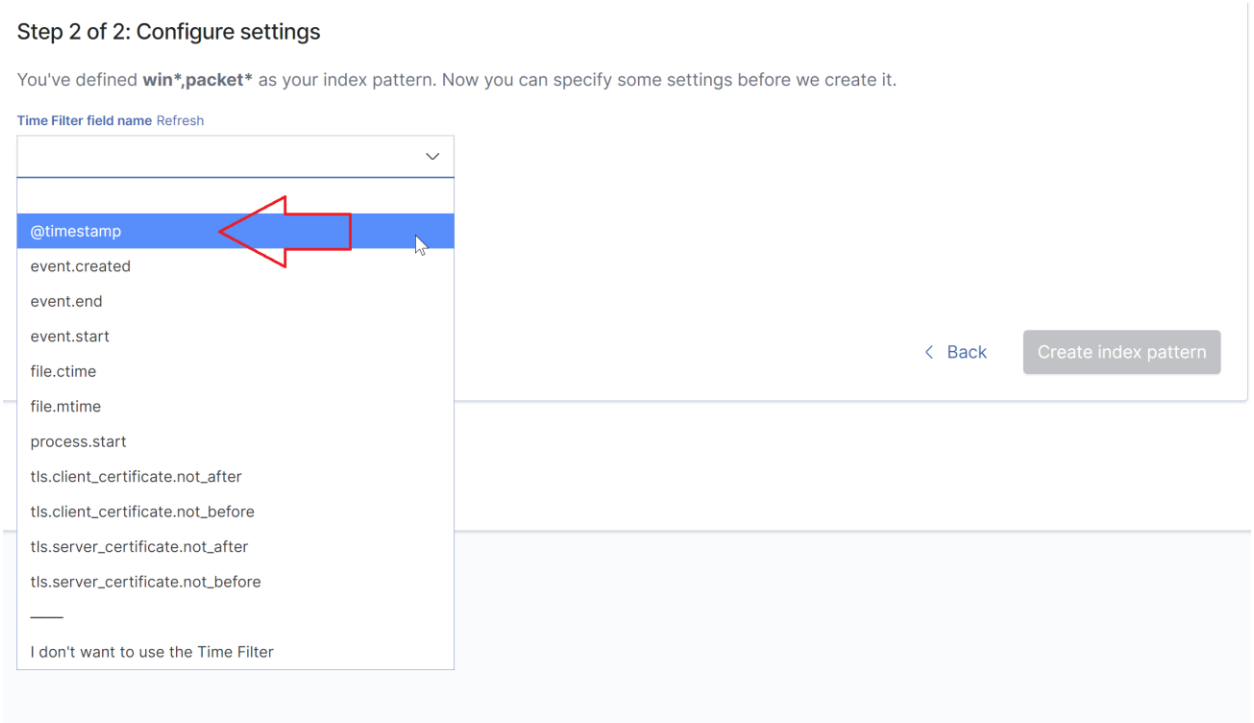
   a. win*,packet*



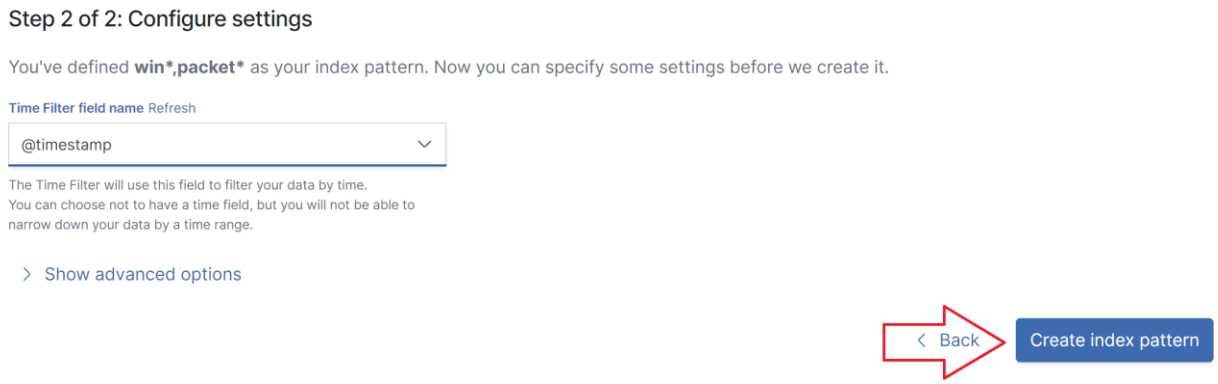
5. Click “Next Step”:



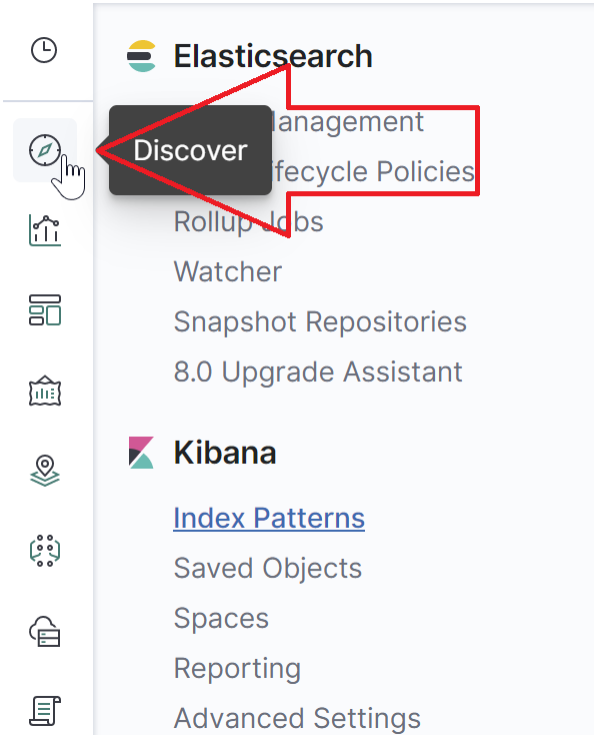
6. For the “Time Filter” choose “@timestamp” from the drop down menu:



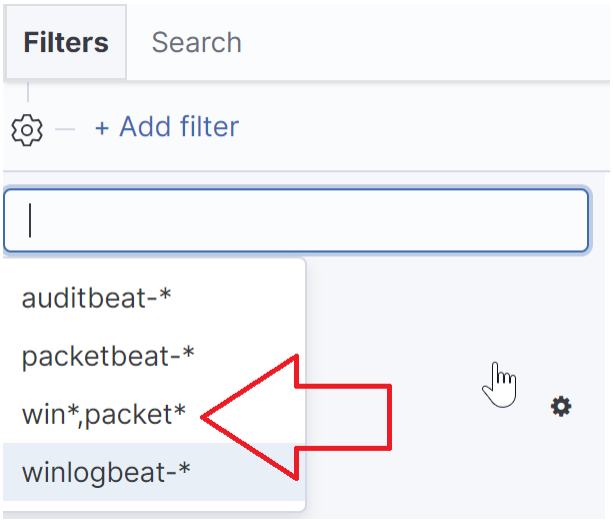
7. Click “Create index pattern”



8. Go to the Kibana Discover tab:



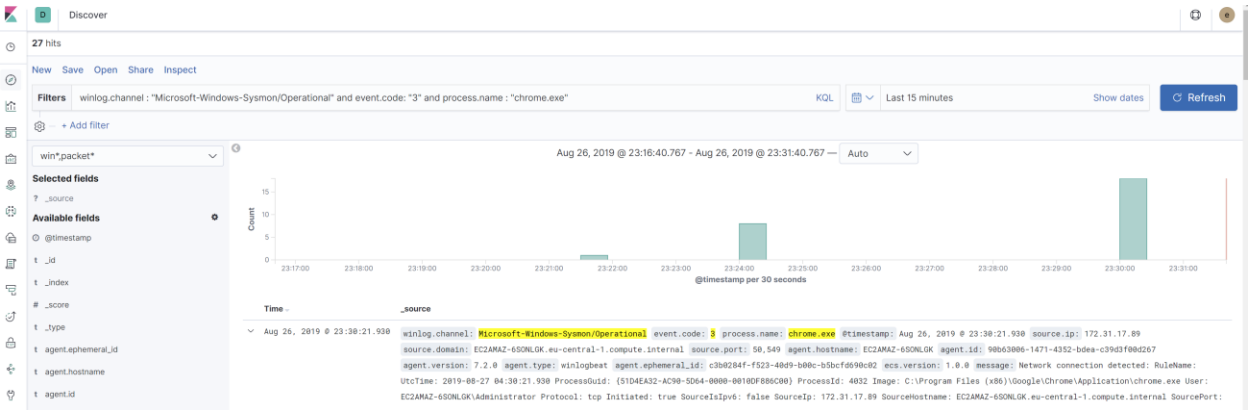
9. In the search pattern drop down choose the newly create search pattern:



10. On your Windows 2016 host use the Chrome web browser to go to a website.

11. In Kibana go back to the Discover tab and type the following KQL query in the search bar and click Update:

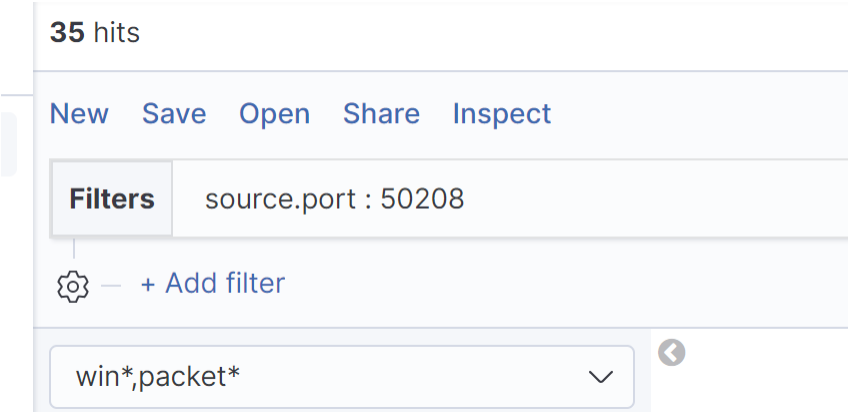
    a. winlog.channel : "Microsoft-Windows-Sysmon/Operational" and event.code: "3" and process.name : "chrome.exe"



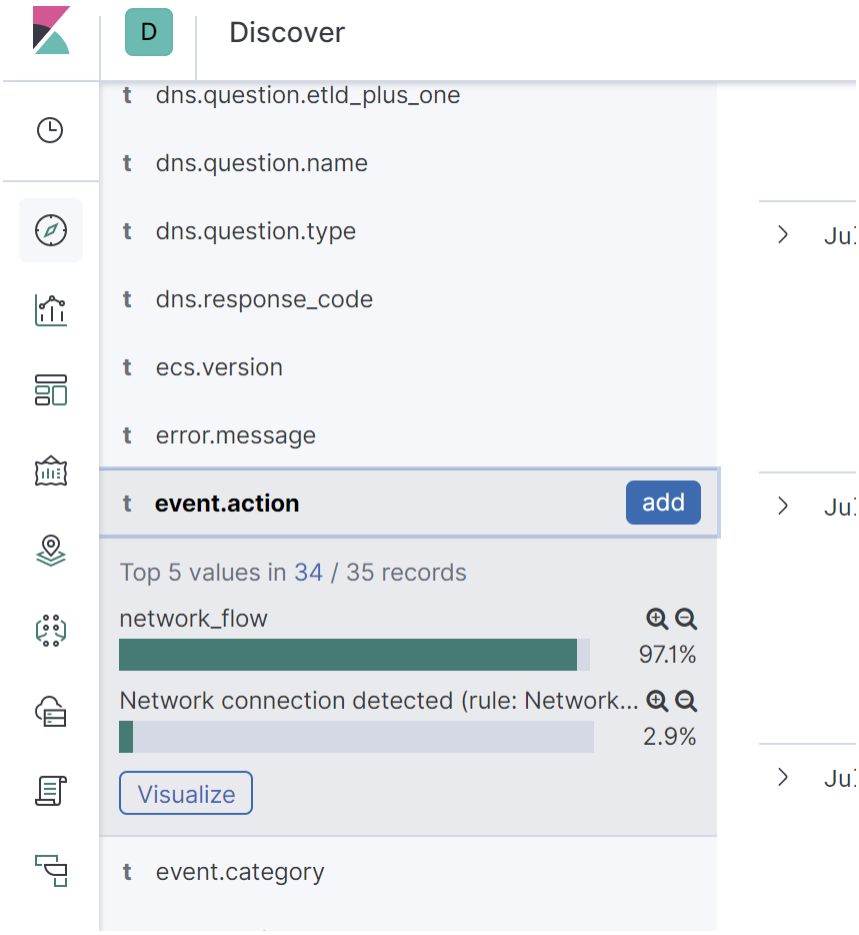
12. Find any event and look for the field ‘source.port’.

13. Go back to the KQL search bar and now type:

    a. source.port : <Port number from step #12>



14. Scroll through the “Selected Fields” on the left and side and look for ‘event.action’ and click on it:



15. You will notice that we matched events from packetbeat, specifically netflow, and winlogbeat, specifically sysmon in a single query. This is implicit correlation.