

Lab 2

Data Ingestion using Beats, Sysmon and MITRE ATT&CK™ configs

Setup Strigo

Your Training Environment

Class URL:


<https://ela.st/elastic-siem-den-lab>

Access Token:


4VML


Lab environment will stay active until 5:00PM MDT


Sign-up to Strigo & Join the classroom ?

 Connect with Google

Or sign-up using your email

Email 

Password 

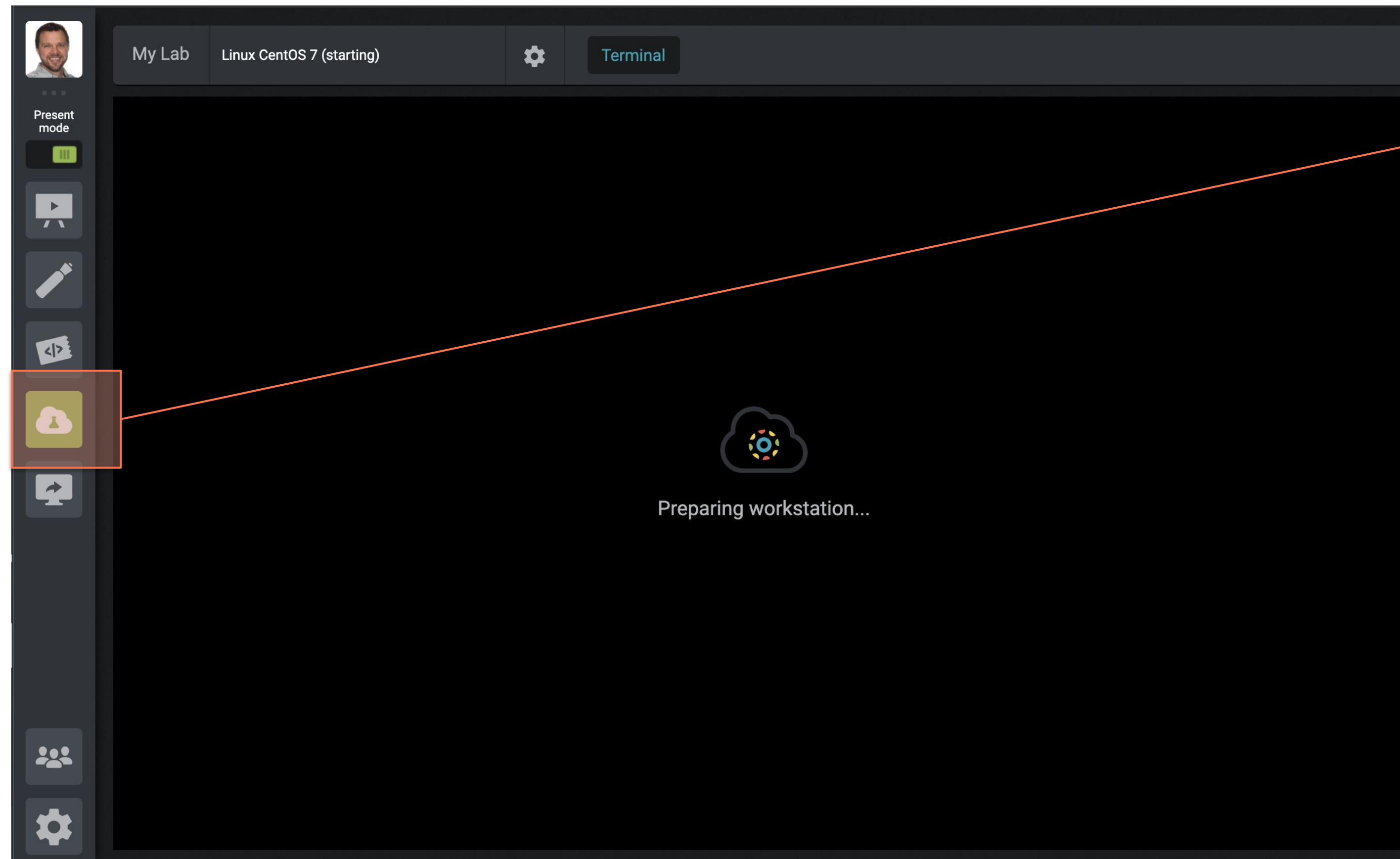
Name 

Sign-up

Already have a Strigo account? [log in here](#)

Linux Beats Scripted Install

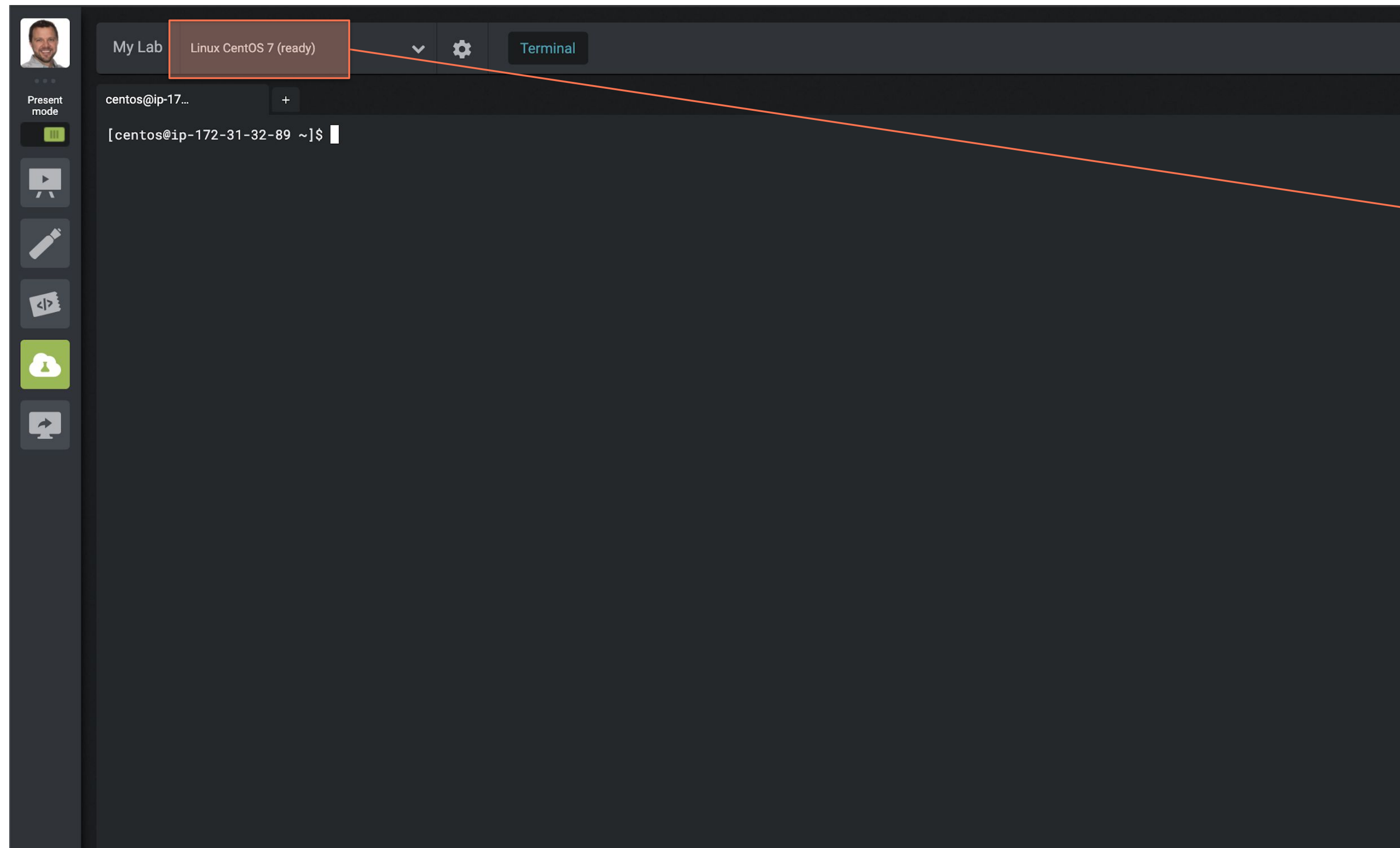
Access “My Lab” (it will take a few minutes)



1 Select 'My Lab'

Linux Beats Scripted Install

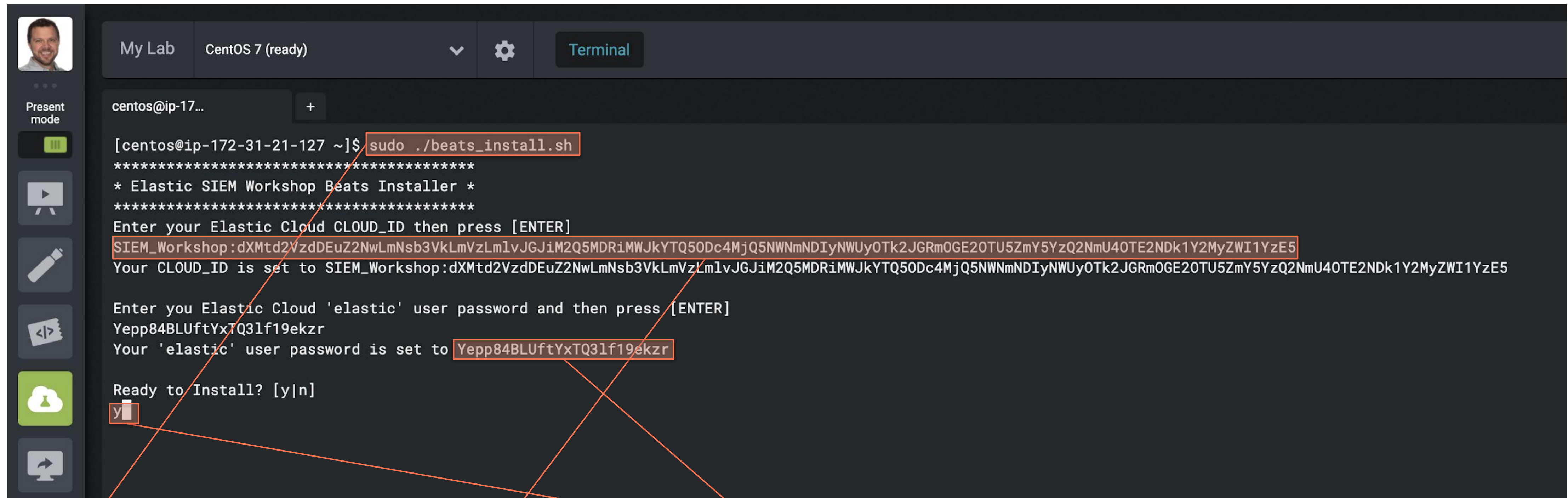
You will see a CentOS Terminal when Lab Instance is Ready



1 After a few minutes, a CentOS Linux instance should be available under 'My Lab'

Linux Beats Scripted Install

Installation of MetricBeat, Filebeat, AuditBeat, Heartbeat and PacketBeat



The screenshot shows a terminal window titled 'My Lab' with 'CentOS 7 (ready)' selected. The terminal output is as follows:

```
centos@ip-17...  
[centos@ip-172-31-21-127 ~]$ sudo ./beats_install.sh  
*****  
* Elastic SIEM Workshop Beats Installer *  
*****  
Enter your Elastic Cloud CLOUD_ID then press [ENTER]  
SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLm1vJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZWl1YzE5  
Your CLOUD_ID is set to SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLm1vJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZWl1YzE5  
  
Enter you Elastic Cloud 'elastic' user password and then press [ENTER]  
Yepp84BLUftYxTQ3lf19ekzr  
Your 'elastic' user password is set to Yepp84BLUftYxTQ3lf19ekzr  
  
Ready to Install? [y|n]  
y
```

Four red lines with numbered circles (1-4) point to specific parts of the terminal output:

- 1 points to the command `sudo ./beats_install.sh`.
- 2 points to the CLOUD_ID value: `SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLm1vJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZWl1YzE5`.
- 3 points to the 'elastic' user password: `Yepp84BLUftYxTQ3lf19ekzr`.
- 4 points to the confirmation 'y' at the bottom.

- 1 Type 'sudo ./beats_install.sh'
- 2 Copy & Paste the CLOUD ID created in Lab 1
- 3 Copy & Paste the 'elastic' user's password created in Lab 1
- 4 Verify values and Type 'y' and [enter]

Linux Beats Scripted Install

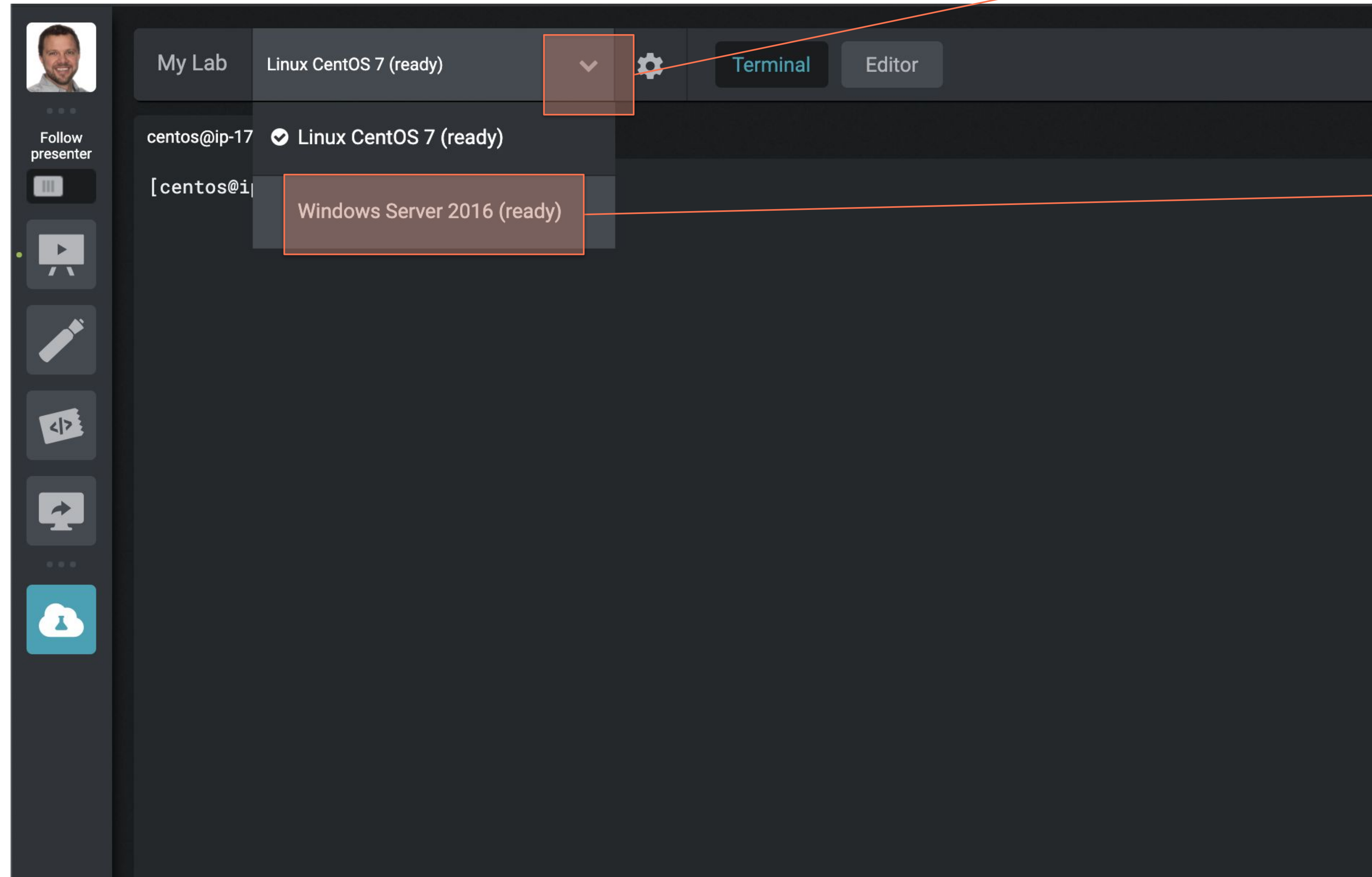
Installation of MetricBeat, Filebeat, AuditBeat, Heartbeat and PacketBeat

For each Elastic Beat, if the installation and communication with your Elastic Cloud Cluster are successful, you should see a message like this:

```
elasticsearch: https://bb3d904b1bda498782495cf4225e2996.us-west1.gcp.cloud.es.io:443...
parse url... OK
connection...
  parse host... OK
  dns lookup... OK
  addresses: 35.199.170.84
  dial up... OK
TLS...
  security: server's certificate chain verification is enabled
  handshake... OK
  TLS version: TLSv1.2
  dial up... OK
talk to server... OK
version: 7.3.1
filebeat setup complete
```

Windows Beats Scripted Install

Access your Windows Server 2016 Instance

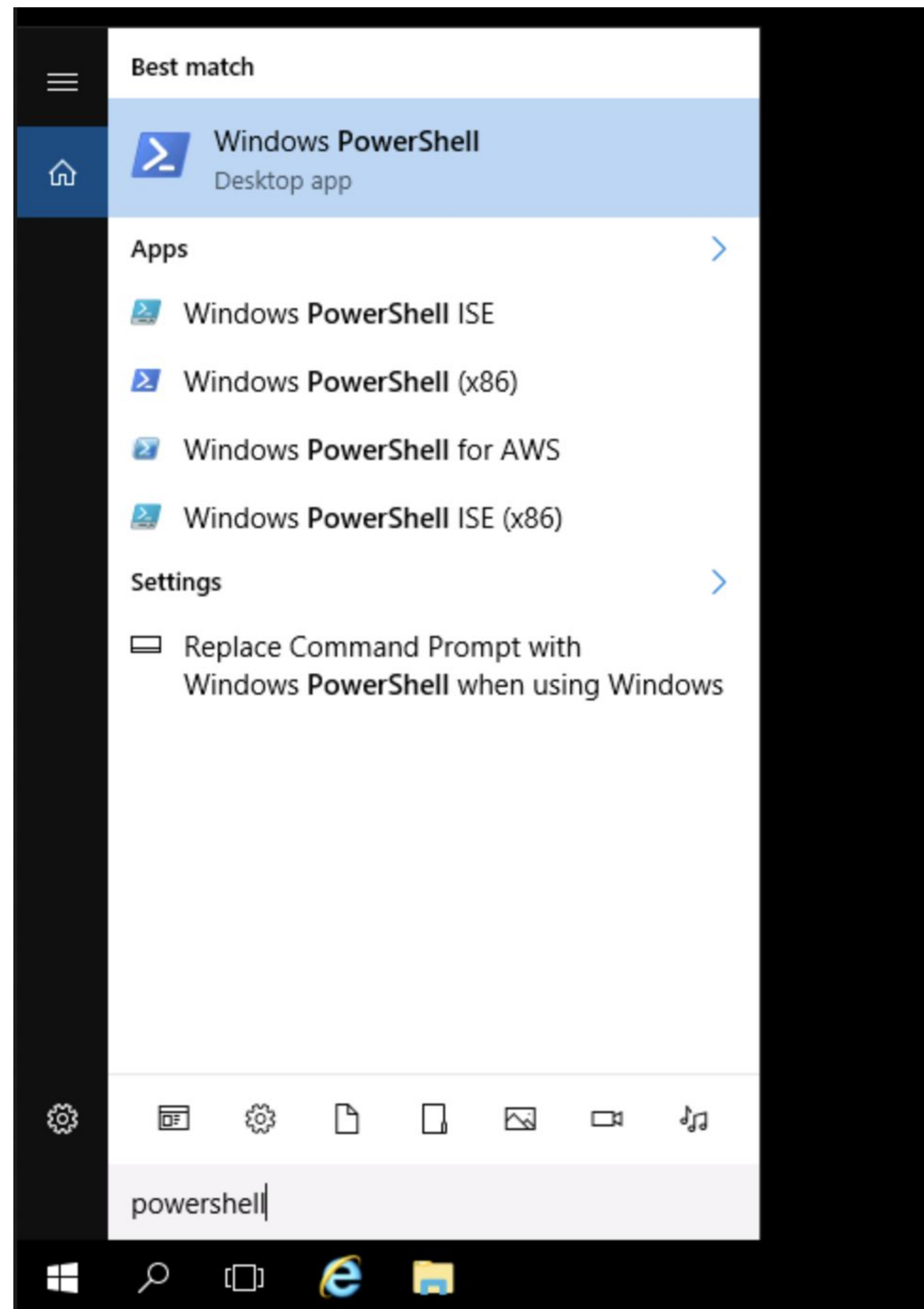


1 Select the arrow next to 'My Lab'

2 Select 'Windows Server 2016'

Windows Scripted Install

Install Sysmon with Custom Config Template



- 1 Type: `cd ela <TAB>` to autocomplete `.\Elastic\` <RETURN/ENTER>
- 2 Type: `sys <TAB>` to autocomplete `'.\sysmon-install.ps1'` <RETURN/ENTER>

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Elastic\
PS C:\Users\Administrator\Elastic> .\sysmon-install.ps1
Installing Sysmon...

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----            8/2/2019 12:55 PM             sysmon-temp

Installation Complete

PS C:\Users\Administrator\Elastic> _
```


Windows Scripted Install

Seamless Clipboard Access using Google Chrome

1 Select the clipboard icon

2 Select Show more

3 Select Learn how

4 Select 'Open Clipboard...'

5 Select Allow

VM Clipboard

Paste text here

Keep open

VM Clipboard

Paste text here

Keep open

The text area above lets you copy and paste content between your local machine and the VM. [Show less](#)

- Copy from your local machine to the VM
Paste content from your local machine into the text area above. You can then paste that content within the VM.
- Copy from the VM to your local machine
Copying content within the VM automatically populates the text area above. You can then copy the content from there to your local machine.

Tip: Users running on Chrome browser can enjoy a seamless copy/paste experience between local and virtual machines. [Learn how](#)

Enable seamless copy/paste functionality

1. Click this link -> [Open Clipboard Permissions](#)

2. Click "Allow" in Chrome's permission dialog

3. You should now be able to seamlessly copy and paste materials between your local machine and the VM.

[Close](#)

app.strigo.io wants to

See text and images copied to the clipboard

[Block](#) [Allow](#)

app.strigo.io wants to

See text and images copied to the clipboard

[Block](#) [Allow](#)

Windows Scripted Install

You must use the Strigo VM Clipboard to Copy Text to the Instance

1 Select the clipboard icon

2 Copy-n-Paste CLOUD ID

3 Type: bea <TAB to autocomplete
.\beats-install.ps1>
<RETURN/ENTER>

4 Copy-n-Paste CLOUD ID and the elastic user's password

VM Clipboard

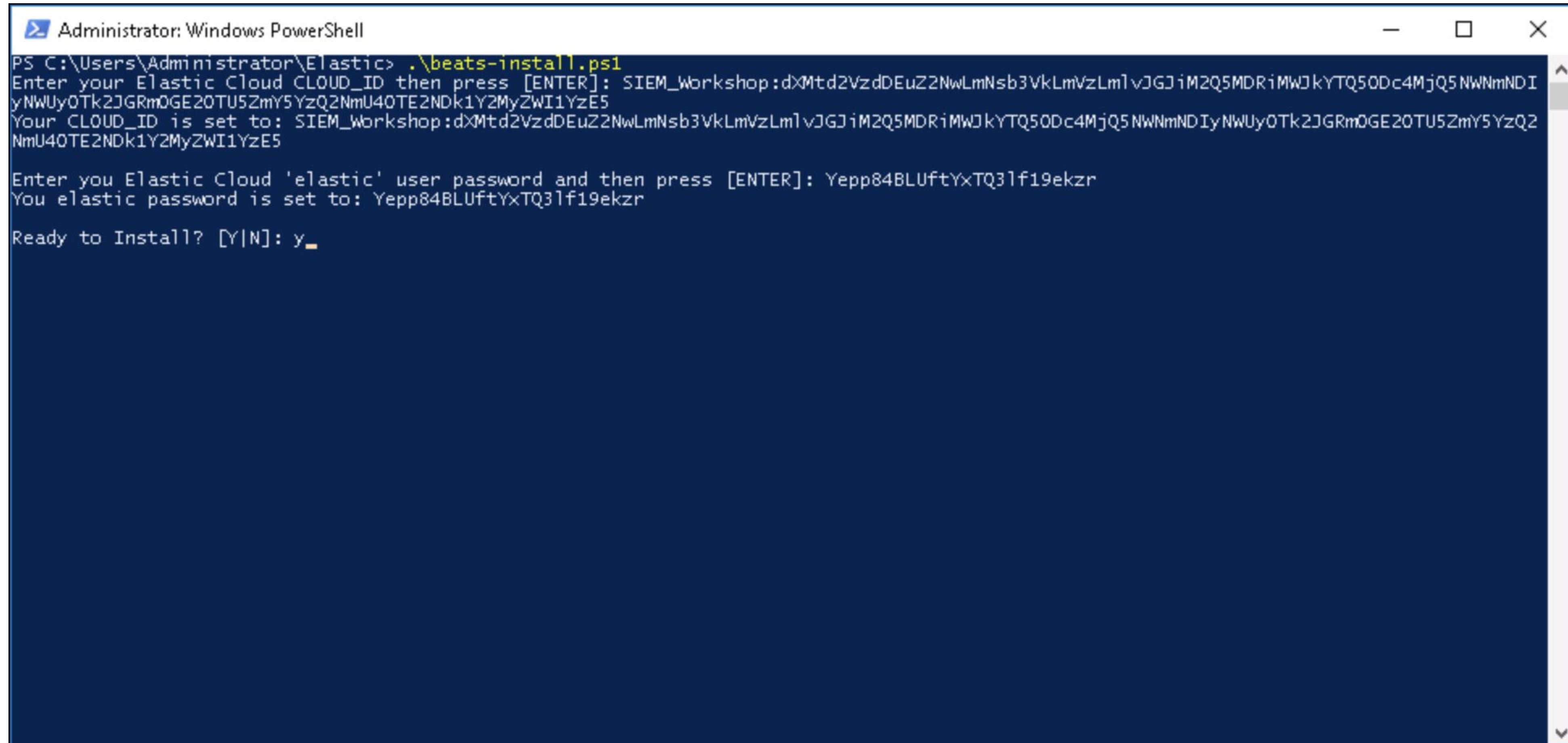
SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZW11YzE5

Administrator: Windows PowerShell

```
Microsoft Corporation. All rights reserved.  
Administrator> cd .\Elastic\  
Administrator\Elastic> .\beats-install.ps1  
Cloud CLOUD_ID then press [ENTER]:
```


Windows Scripted Install

Winlogbeat & Metricbeat Installation



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Elastic> .\beats-install.ps1
Enter your Elastic Cloud CLOUD_ID then press [ENTER]: SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmIvJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZWl1YzE5
Your CLOUD_ID is set to: SIEM_Workshop:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmIvJGJiM2Q5MDRiMWJkYTQ5ODc4MjQ5NWNmNDIyNWUyOTk2JGRmOGE2OTU5ZmY5YzQ2NmU4OTE2NDk1Y2MyZWl1YzE5

Enter you Elastic Cloud 'elastic' user password and then press [ENTER]: Yepp84BLUftYxTQ3lf19ekzr
You elastic password is set to: Yepp84BLUftYxTQ3lf19ekzr

Ready to Install? [Y|N]: y_
```

What does it mean to install a Beat?

i.e., What did the installation scripts do?

- Download and install the Beat artifact (e.g., yum, or from elastic.co)
- Update the configuration files (e.g., filebeat.yml, auditbeat.yml, etc.)
- Create a keystore and add CLOUD_ID and CLOUD_AUTH
- Perform the Beat setup to push content to Elasticsearch and Kibana

```
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
```

- Start the Beat service

ATT&CK™ Beats Community

ATT&CK™ Configs Thanks to the Community

- olafhartong / sysmon-modular
- bfuzzy / auditd-attack

olafhartong / sysmon-modular

Watch 85

Code

Issues 0

Pull requests 0

Projects 0

Wiki

Security

Insights

A repository of sysmon configuration m

sysmon

dfir

threat-hunting

mitre-a

203 commits

3

Branch: master

New pull request

olafhartong

several updates

10_process_access

11_file_create

12_13_14_registry_event

15_file_create_stream_hash

17_18_pipe_event

19_20_21_wmi_event

1_process_creation

2_file_create_time

bfuzzy / auditd-attack

Watch 38

Stars

Code

Issues 1

Pull requests 0

Projects 0

Wiki

Security

Insights

A Linux Auditd rule set mapped to MITRE's Attack Framework

auditd

attack-detection

mitre-attack

threat-hunting

linux

31 commits

1 branch

0 releases

1 contributor

Branch: master

New pull request

Create new file

Upload files

Find Fil

bfuzzy

Commented out Ignoring SELinux IT IS bad practice

Latest commit

LICENSE

Initial commit

README.md

Update README.md

attack_map.png

Updated ATT&CK Mappings

auditd-attack.rules

Commented out Ignoring SELinux IT IS bad practice

base_config.rules

base config

layer-2.json

Updated ATT&CK Mapping

README.md

auditd-attack

A Linux Auditd rule set mapped to MITRE's Attack Framework