Lab 2

Data Ingestion using Beats and MITRE ATT&CK™

elastic

Setup Strigo

Your Training Environment

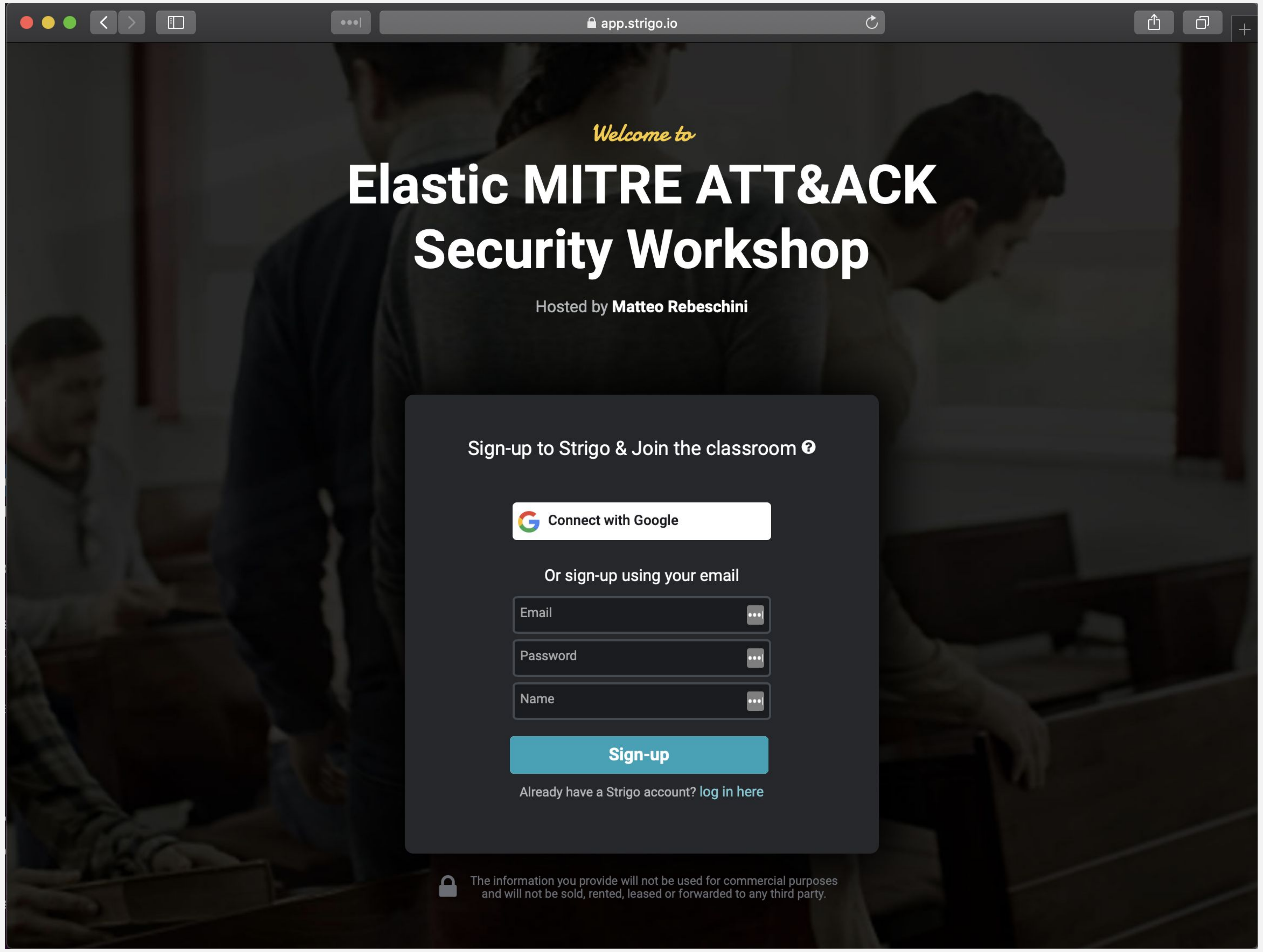
Class URL:

https://bit.ly/BSidesLV2019

Access Token:

YK7M

Lab environment will stay active until 8/10 @ 5:00PM



Welcome to

Elastic MITRE ATT&ACK Security Workshop

Hosted by **Matteo Rebeschini**

Sign-up to Strigo & Join the classroom

Or sign-up using your email

Email

Password

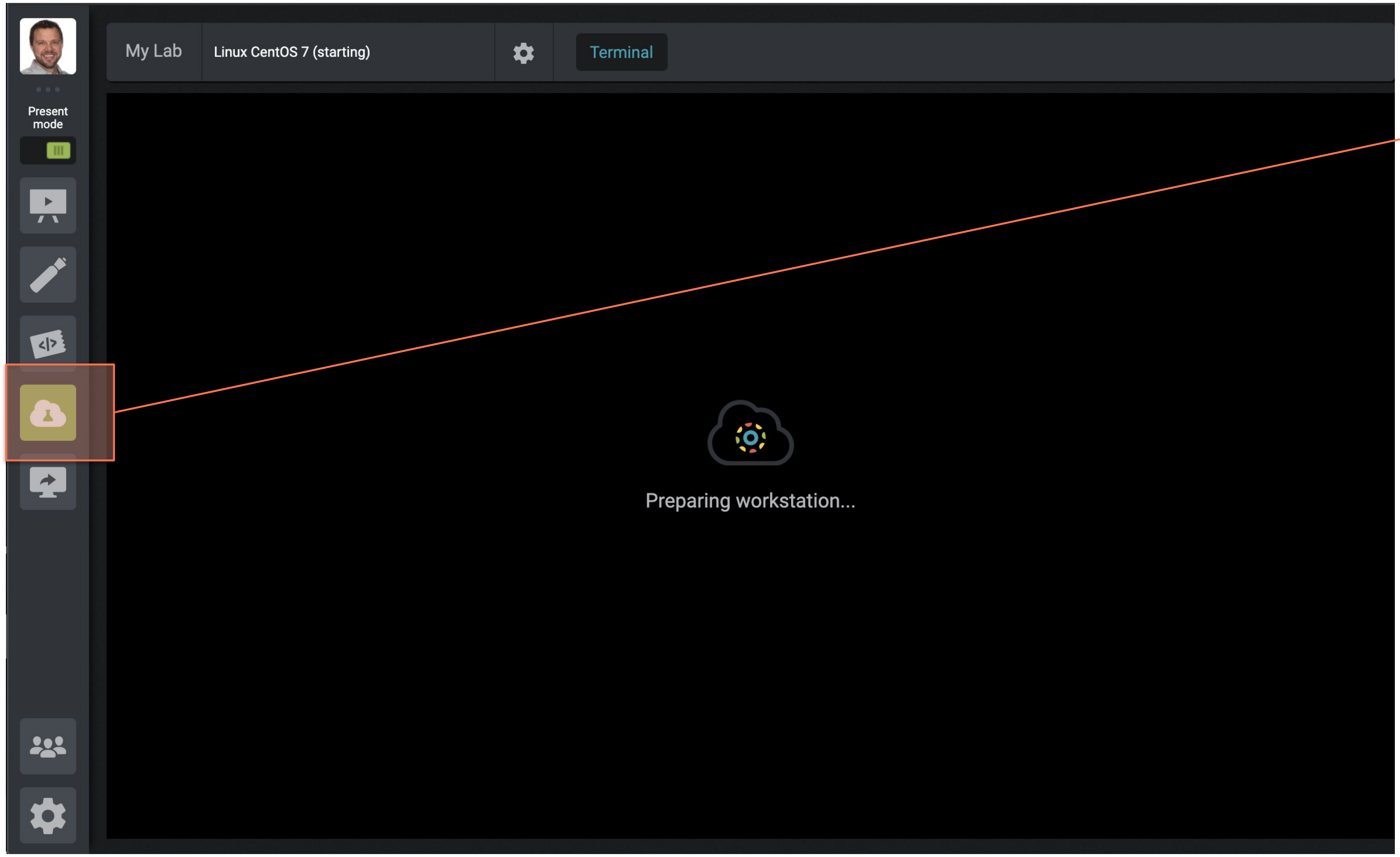
Name

Already have a Strigo account? log in here

The information you provide will not be used for commercial purposes and will not be sold, rented, leased or forwarded to any third party.

Linux Beats Scripted Install

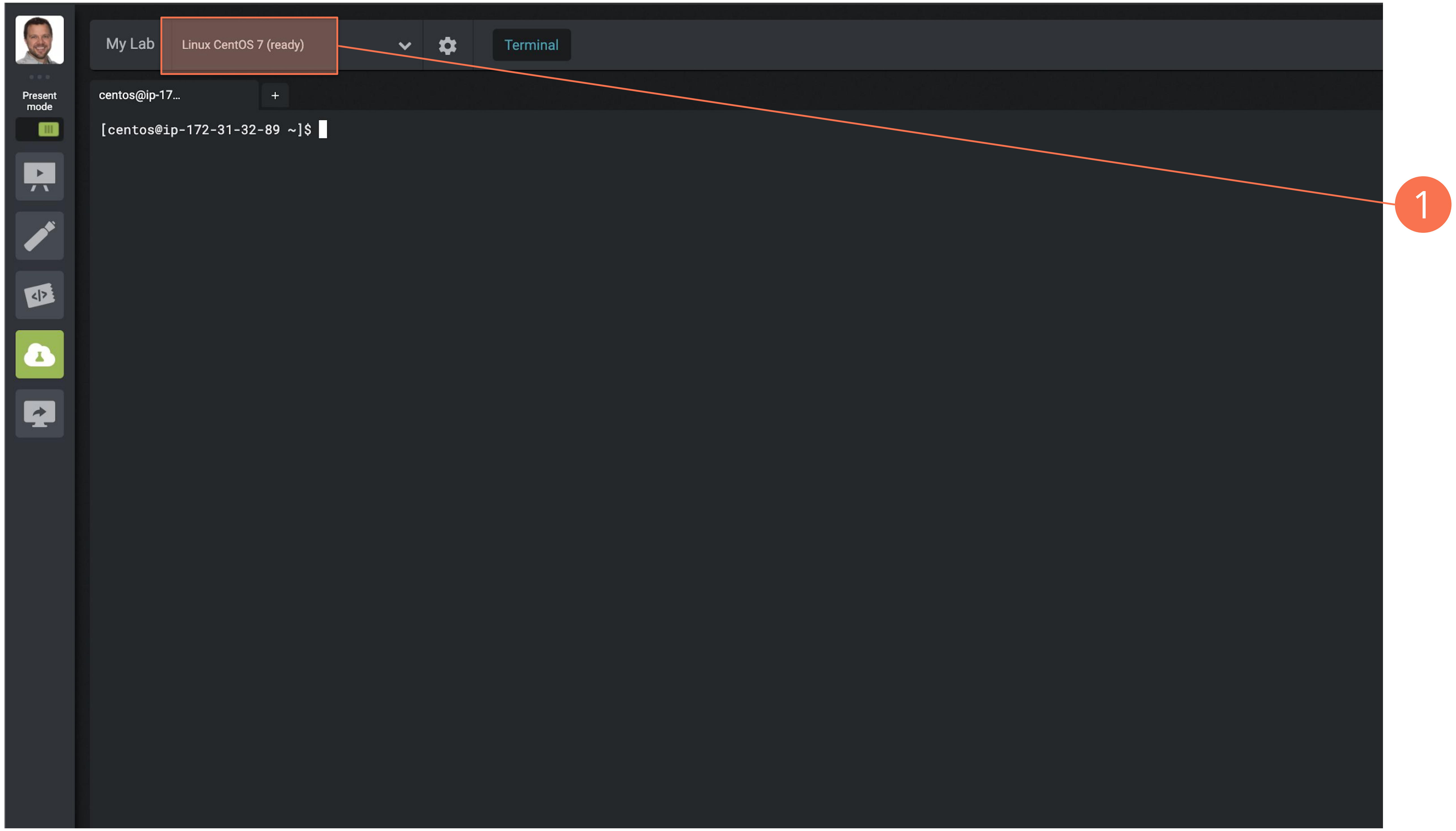
Access “My Lab” (it will take a few minutes)



1 Select ‘My Lab’

Linux Beats Scripted Install

You will see a CentOS Terminal when Lab Instance is Ready



```
[centos@ip-172-31-32-89 ~]$
```

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

Linux Beats Scripted Install

Installation of MetricBeat, Filebeat, AuditBeat and PacketBeat

My Lab
Linux CentOS 7 (ready)
Terminal
Present mode
centos@ip-17...
+

```
[centos@ip-172-31-32-89 ~]$ ./beats_install.sh
Enter your Elastic Cloud CLOUD_ID then press [ENTER]
bsides-test:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJDFkZmI5NGNlN2JjZDQxNDA4NmYwZGM0OGM5YjY0Y2QxJDdhMjk0ZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz
Your CLOUD_ID is set to bsides-test:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJDFkZmI5NGNlN2JjZDQxNDA4NmYwZGM0OGM5YjY0Y2QxJDdhMjk0ZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz


Enter you Elastic Cloud 'elastic' user password and then press [ENTER]
TunqACasd0ZAP7w4GMnuO3PY
Your elastic password is set to TunqACasd0ZAP7w4GMnuO3PY


Ready to Install? [y|n]
```

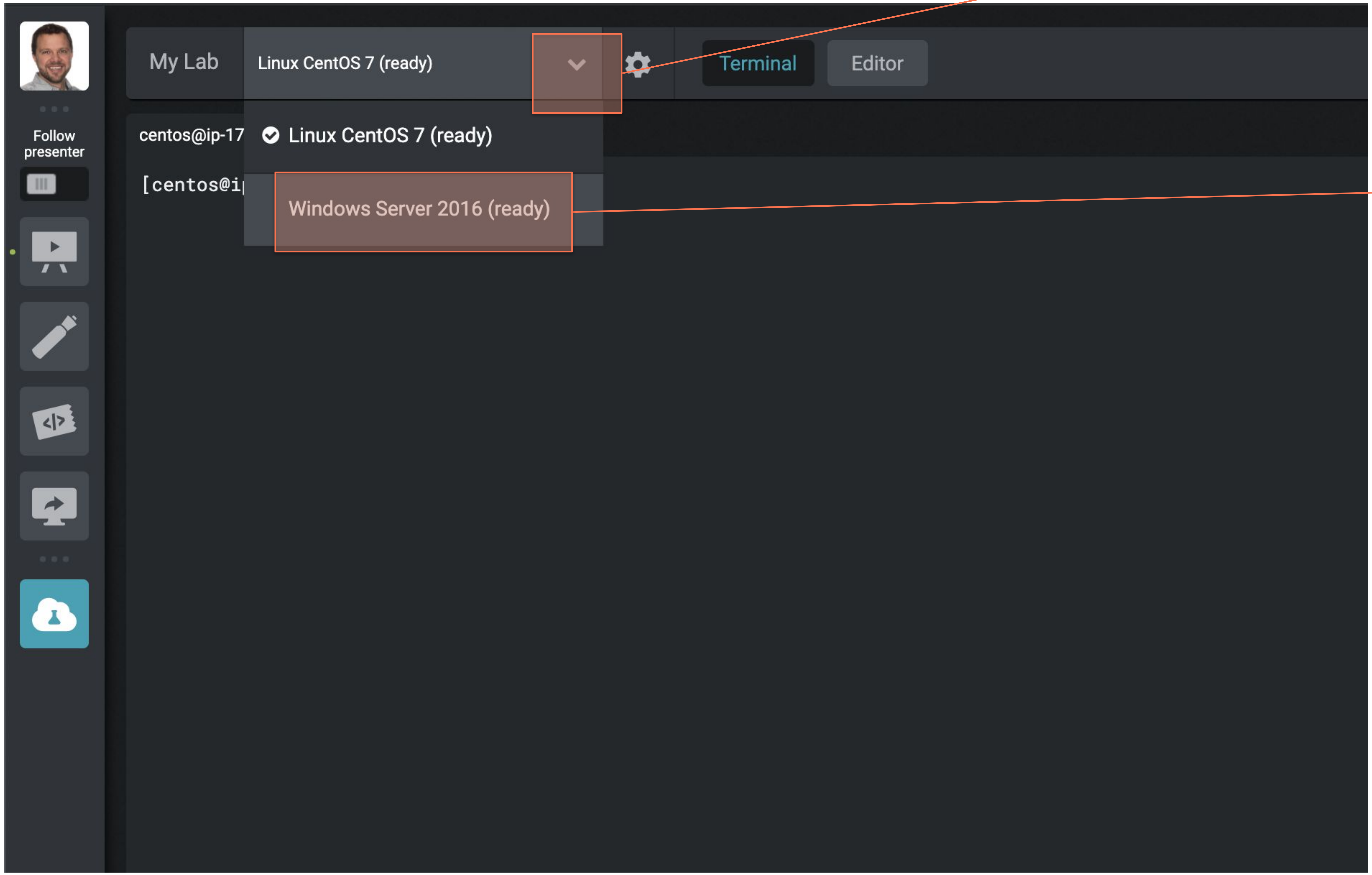
1 Type './beats_install.sh'

2 Copy-n-Paste the CLOUD ID created in Lab 1

3 Copy-n-Paste the elastic user's password created in Lab 1

Windows Beats Scripted Install

Access your Windows Server 2016 Instance

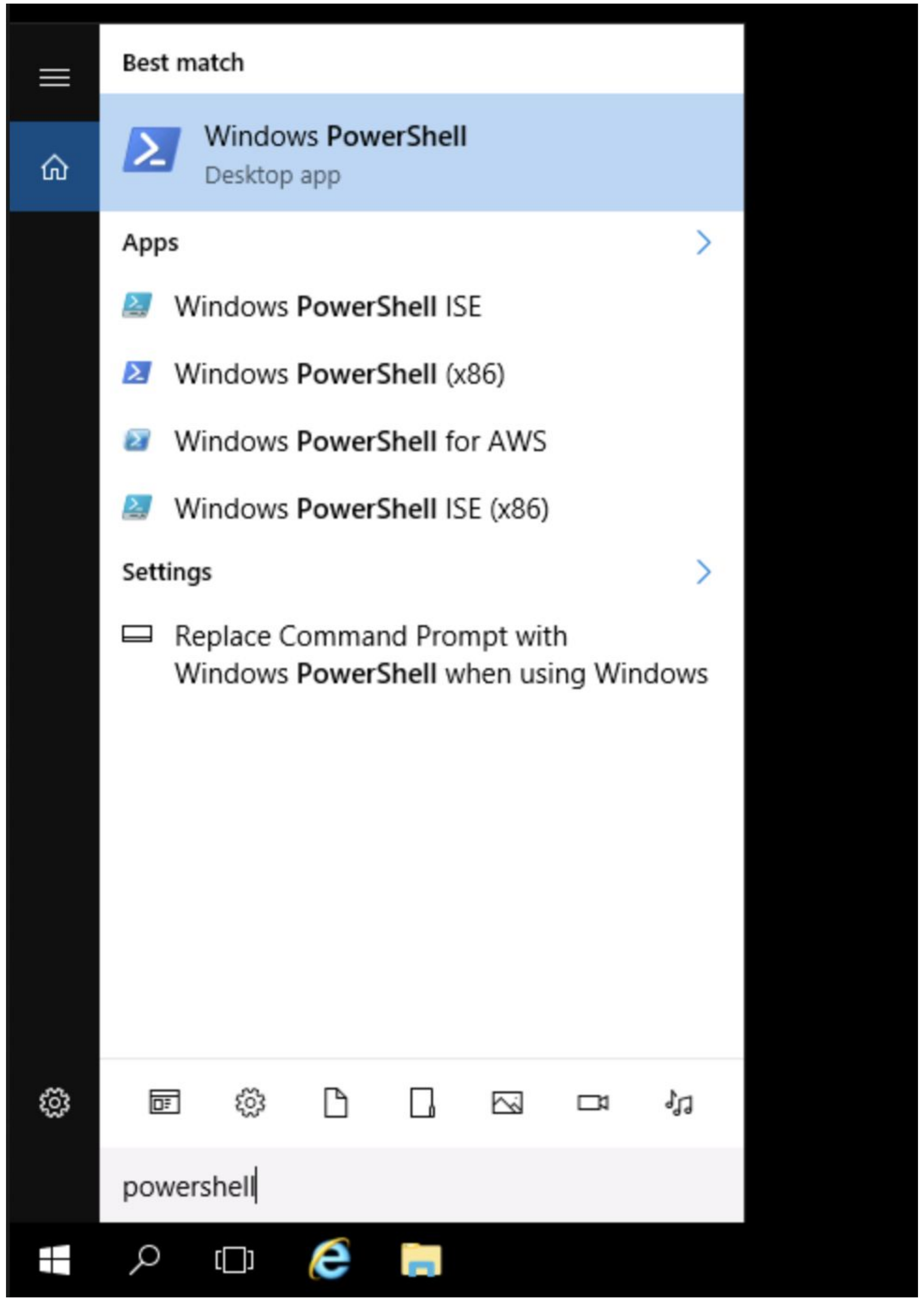


1 Select the arrow next to ‘My Lab’

2 Select ‘Windows Server 2016’

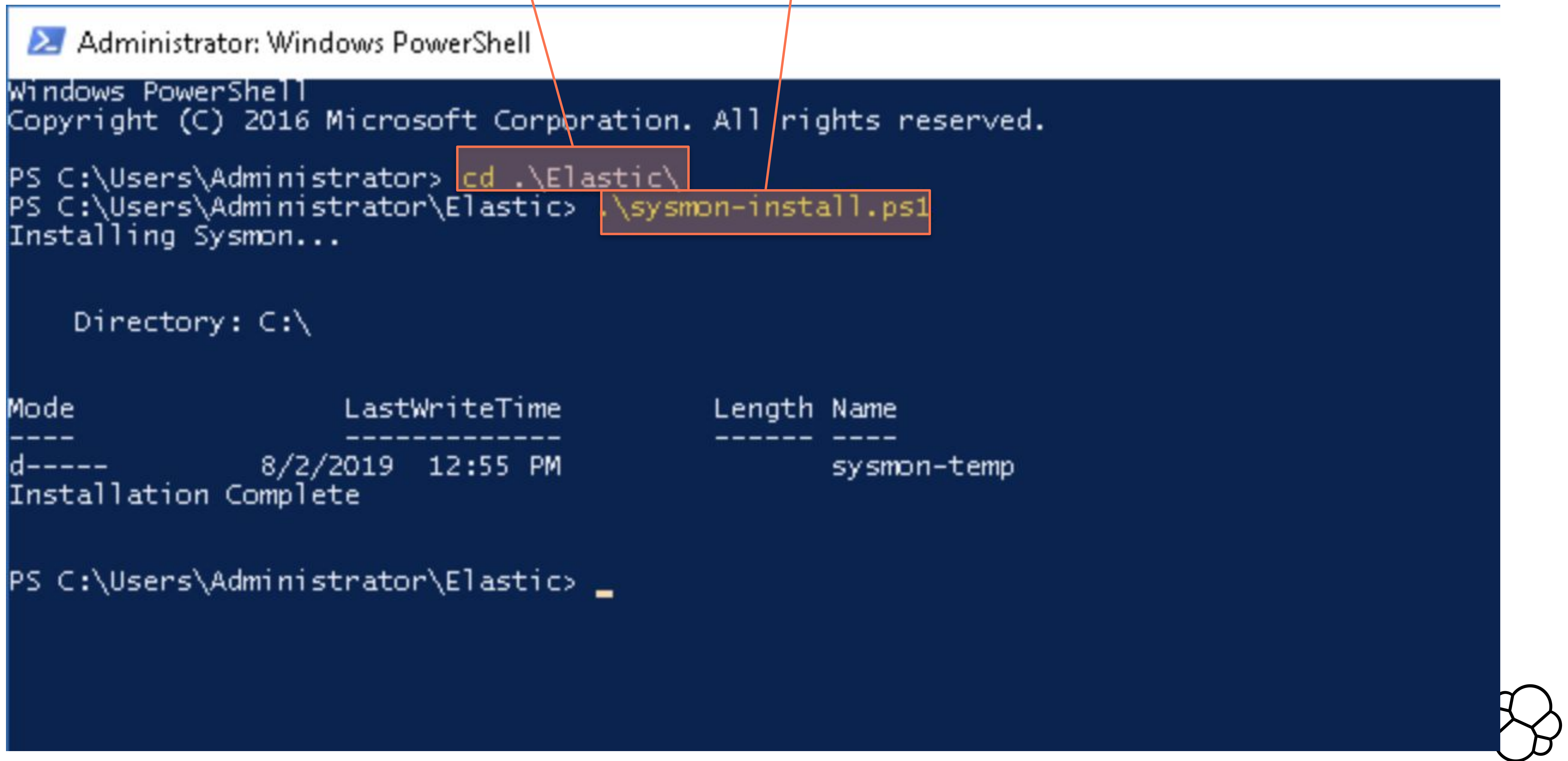
Windows Scripted Install

Install Sysmon with Custom Config Template


Best match
Windows PowerShell
Desktop app
Apps
Windows PowerShell ISE
Windows PowerShell (x86)
Windows PowerShell for AWS
Windows PowerShell ISE (x86)
Settings
Replace Command Prompt with Windows PowerShell when using Windows
powershell

1 Type: cd ela <TAB> to autocomplete .\Elastic\> <RETRUN/ENTER>

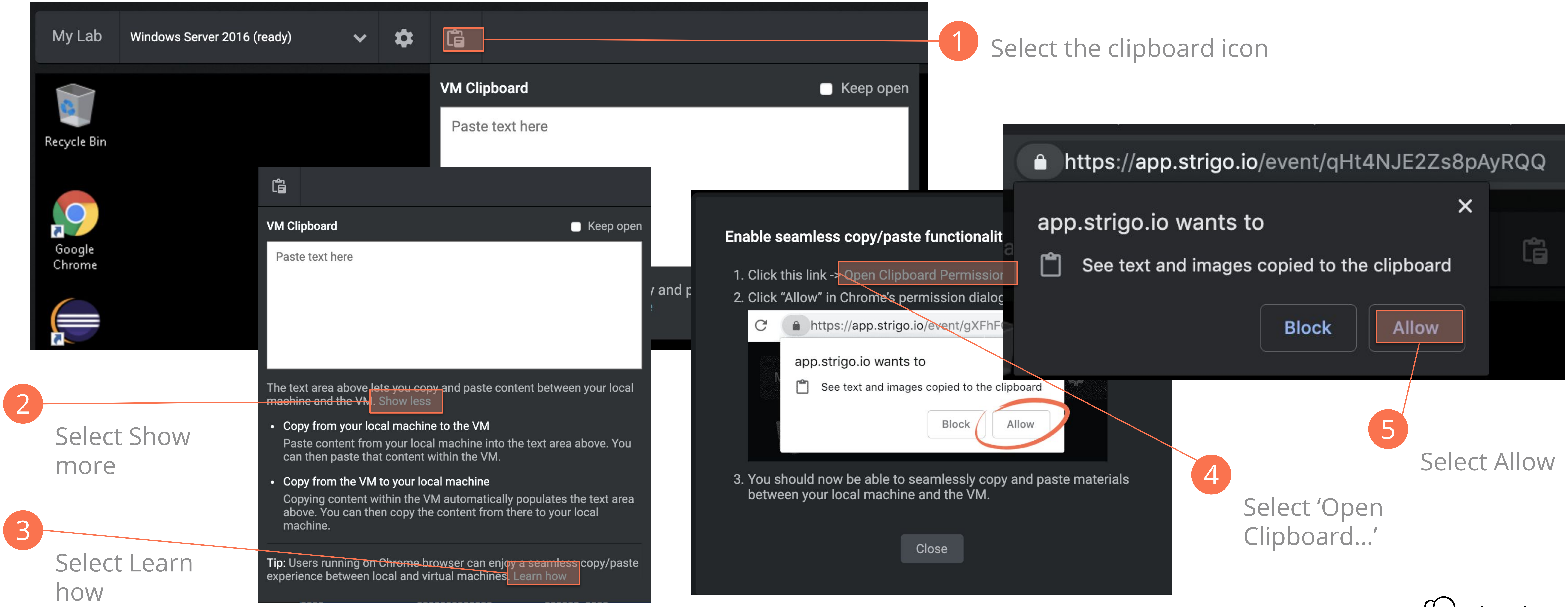
2 Type: sys <TAB> to autocomplete ‘.\sysmon-install.ps1’ <RETURN/ENTER>



```
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



VM Clipboard ☐ Keep open

Paste text here

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 functionalit

1. Click this link -> Open Clipboard Permissior
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

https://app.strigo.io/event/gXFhF

app.strigo.io wants to

See text and images copied to the clipboard

Block Allow

https://app.strigo.io/event/qHt4NJE2Zs8pAyRQQ

app.strigo.io wants to

See text and images copied to the clipboard

Block Allow

1 Select the clipboard icon

2 Select Show more

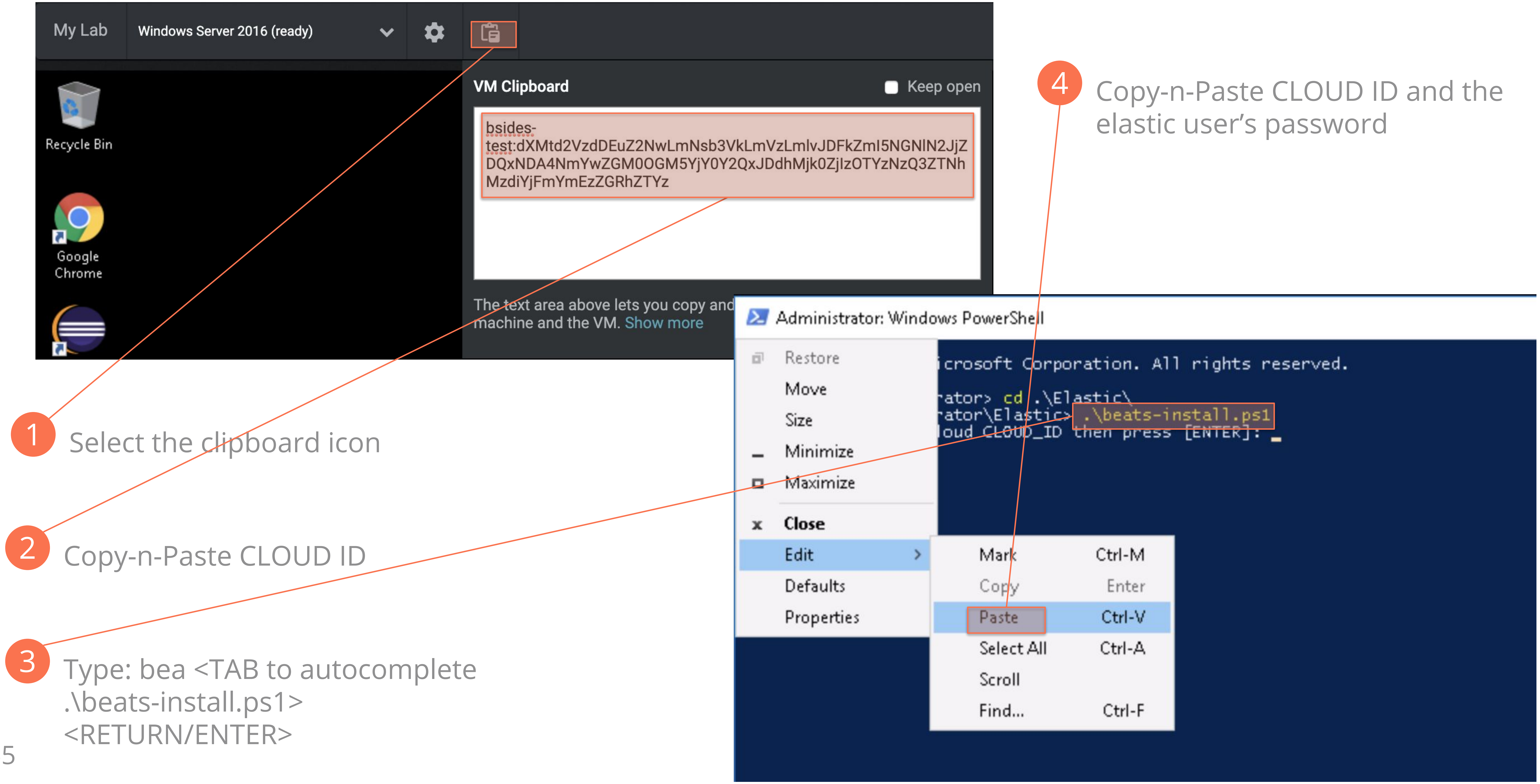
3 Select Learn how

4 Select 'Open Clipboard...'

5 Select Allow

Windows Scripted Install

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



VM Clipboard

□ Keep open

```
bsides-
test:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJDFkZmI5NGNlN2JjZ
DQxNDA4NmYwZGM0OGM5YjY0Y2QxJDdhMjk0ZjIzOTYzNzQ3ZTNh
MzdiYjFmYmEzZGRhZTYz
```

The text area above lets you copy and machine and the VM. Show more

```
icrosoft Corporation. All rights reserved.

rator> cd .\Elastic\
rator\Elastic> .\beats-install.ps1
loud CLOUD_ID then press [ENTER]: _
```

1 Select the clipboard icon

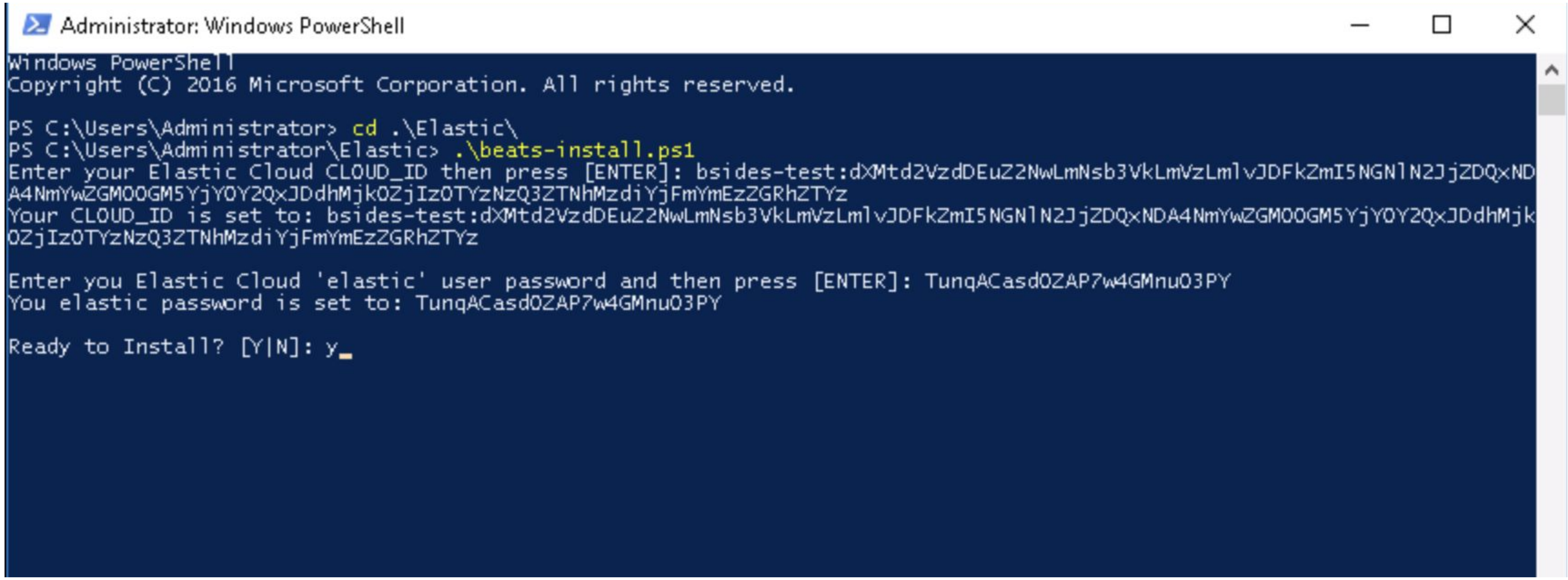
2 Copy-n-Paste CLOUD ID

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

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

Windows Scripted Install

Winlogbeat & Metricbeat Installation



Administrator: Windows PowerShell

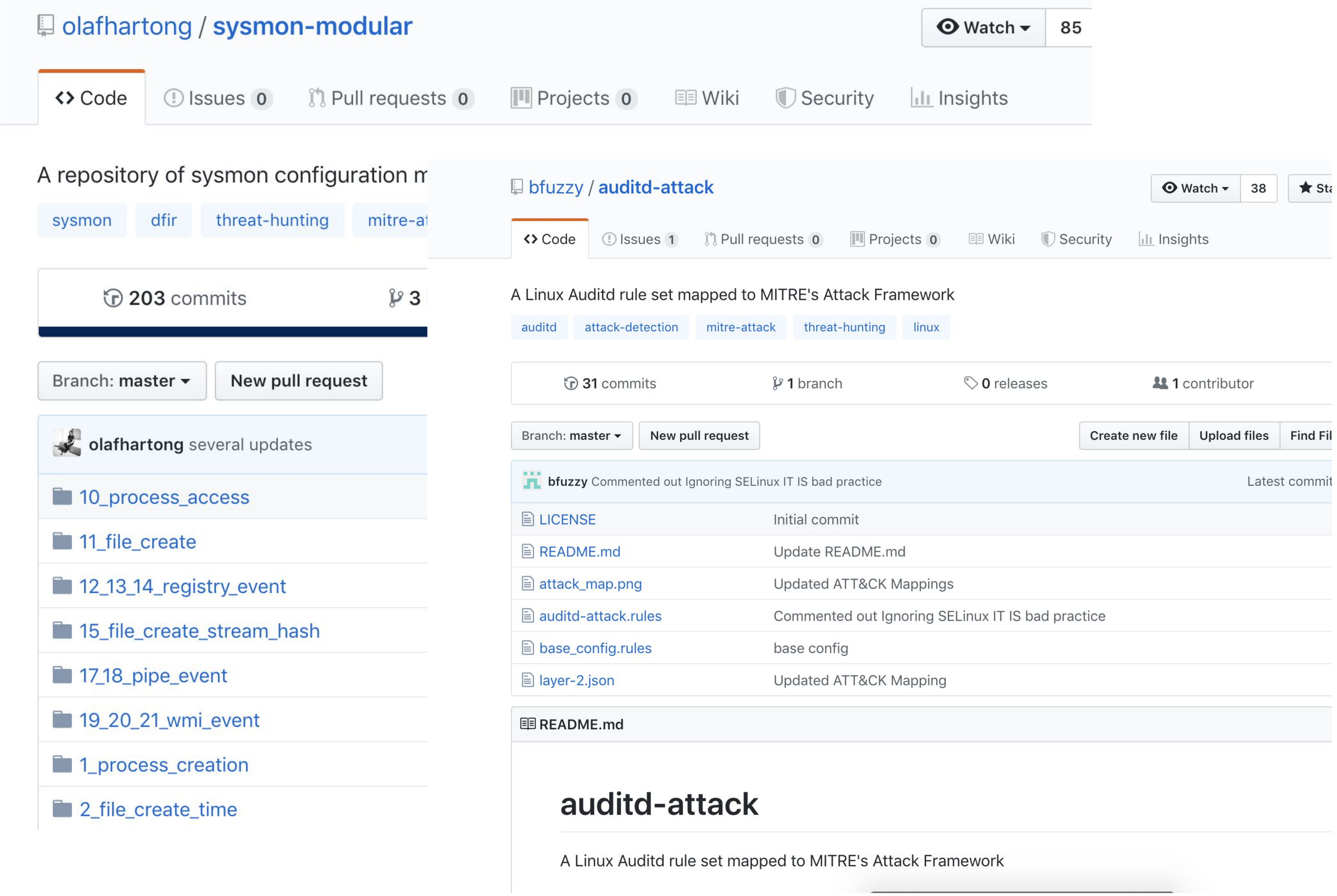
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Elastic\
PS C:\Users\Administrator\Elastic> .\beats-install.ps1
Enter your Elastic Cloud CLOUD_ID then press [ENTER]: bsides-test:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJDFkZmI5NGNlN2JjZDQxND
A4NmYwZGMOOGM5YjYOY2QxJDdhMjkOZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz
Your CLOUD_ID is set to: bsides-test:dXMtd2VzdDEuZ2NwLmNsb3VkLmVzLmlvJDFkZmI5NGNlN2JjZDQxNDA4NmYwZGMOOGM5YjYOY2QxJDdhMjk
OZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz

Enter you Elastic Cloud 'elastic' user password and then press [ENTER]: TunqACasdOZAP7w4GMnuO3PY
You elastic password is set to: TunqACasdOZAP7w4GMnuO3PY

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

ATT&CK™ Beats Community

ATT&CK™ configs Thanks to the community

- olafhartong / sysmon-modular

- bfuzzy / auditd-attack



A repository of sysmon configuration m

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

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

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