# Blue Team: Summary of Operations

Report by **Paul Barrett**

**CyberSecurity Analyst**

Version 1 **20th December 2020**

Version 2 **12th January 2020**

## 

## **Table of Contents**

* Network Topology \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 3
* Description of Targets \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 4
* Monitoring the Targets \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 5
* Patterns of Traffic and Behavior \_\_\_\_\_\_\_\_\_\_\_ Page 6
* Suggestions for Going Further \_\_\_\_\_\_\_\_\_\_\_\_ Page 7
* Screenshots Used as Evidence \_\_\_\_\_\_\_\_\_\_\_ Page 8

## 

## **Network Topology**

|  |  |
| --- | --- |
| **Network** | **Machines** |
| Address Range: **192.168.1.1/24**  Netmask: **255.255.255.0**  Gateway: **10.0.0.1** | IPv4: **192.168.1.1**  OS: Microsoft **Windows 10**  Hostname: ML-RefVm-684427  **Azure Host Machine** |
| IPv4: **192.168.1.90**  OS: Kali Linux 5.4.0  Hostname: **Kali**  **(Attack Machine)** |
| IPv4: **192.168.1.100**  OS: Ubuntu Linux  Hostname: ELK Stack |
| IPv4: **192.168.1.110**  OS: **Linux 3.16.0-6-amd64**  Hostname: **TARGET1** |
| IPv4: **192.168.1.115**  OS: **Linux 3.16.0-6-amd64**  Hostname: **TARGET2** |



## Description of Targets

Fill in the following:

* Two VMs on the network were vulnerable to attack:
  + **Target 1** [IP Address **192.168.1.110**]
  + **Target 2** [IP Address **192.168.1.115**]
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

## 

## **Monitoring the Targets**

This scan identifies the services below as potential points of entry:

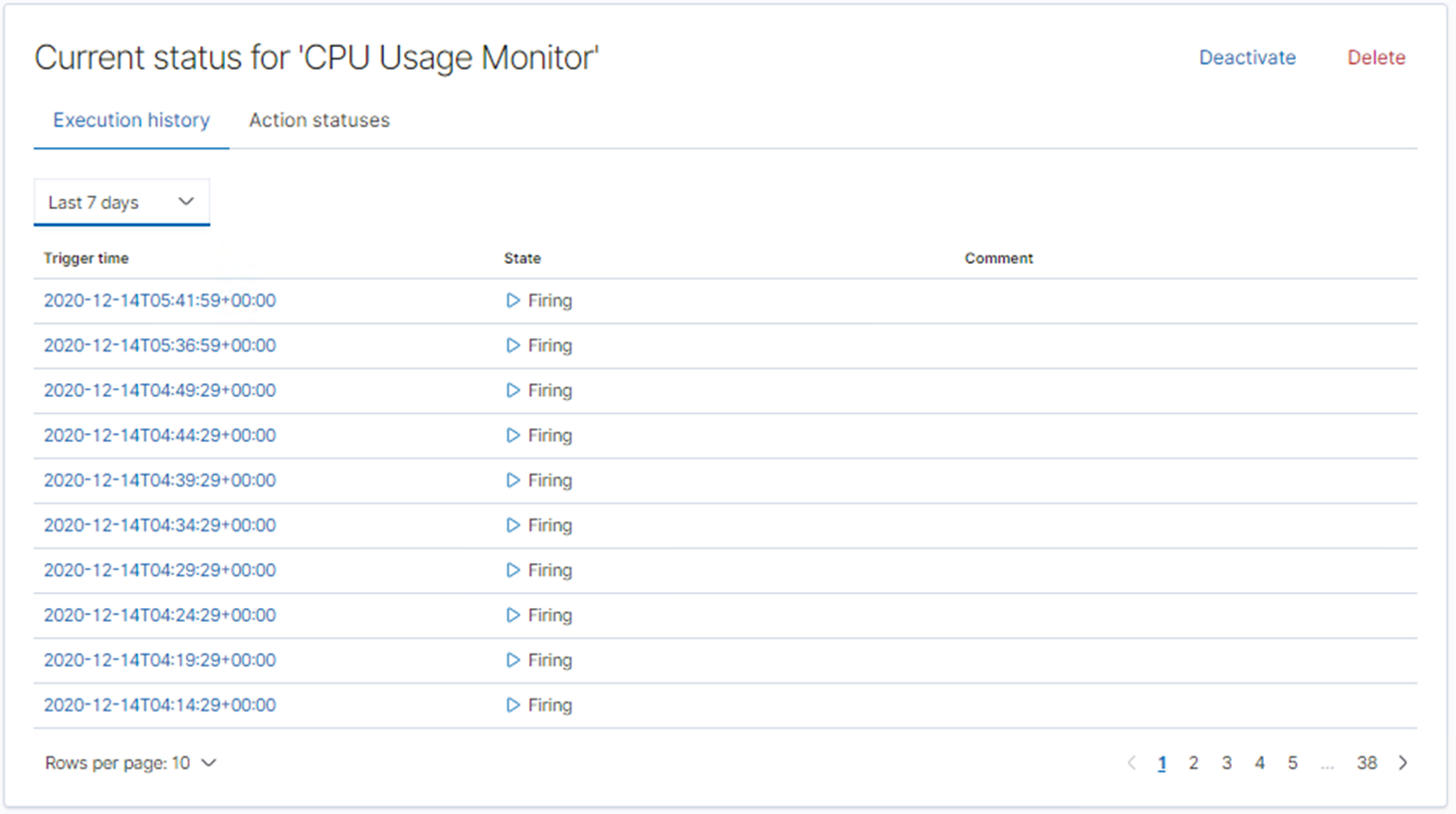
* **Target 1**
  + List of
  + Potentially vulnerable
  + Services
* **Target 2**
  + List of
  + Potentially vulnerable
  + Services

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**Kibana Watcher Alert 1: CPU Usage Monitor**

**CPU Usage Monitor** is implemented as follows:

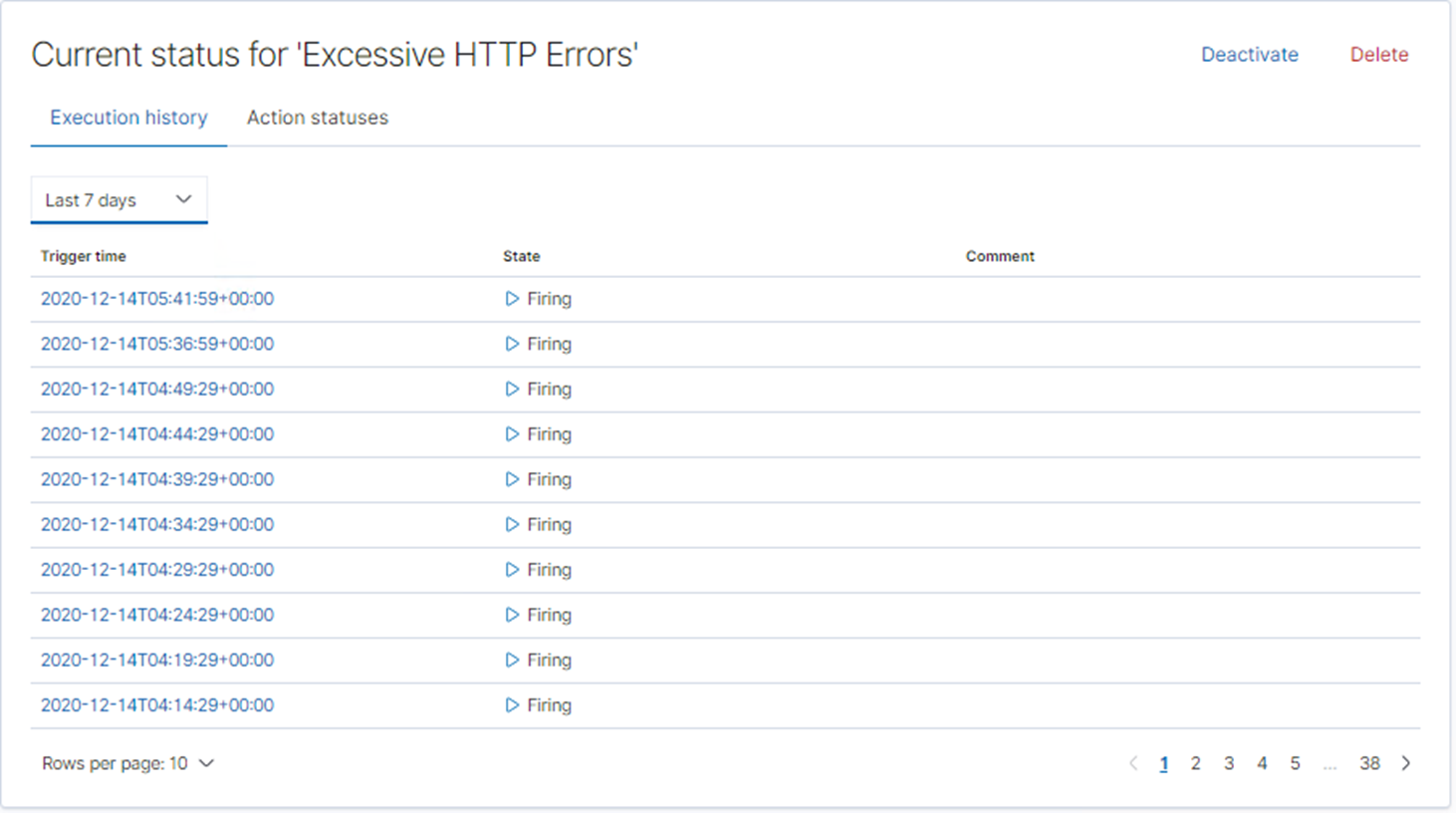
* This metric measures CPU usage
* The alert is instructed to run a watch every minute
* The alert sends a trigger when the percentage of CPU usage is above 0.25 in a 5-minute window.



**Kibana Waterch Alert 2: Excessive HTTP Errors**

**Excessive HTTP Errors Monitor** is implemented as follows:

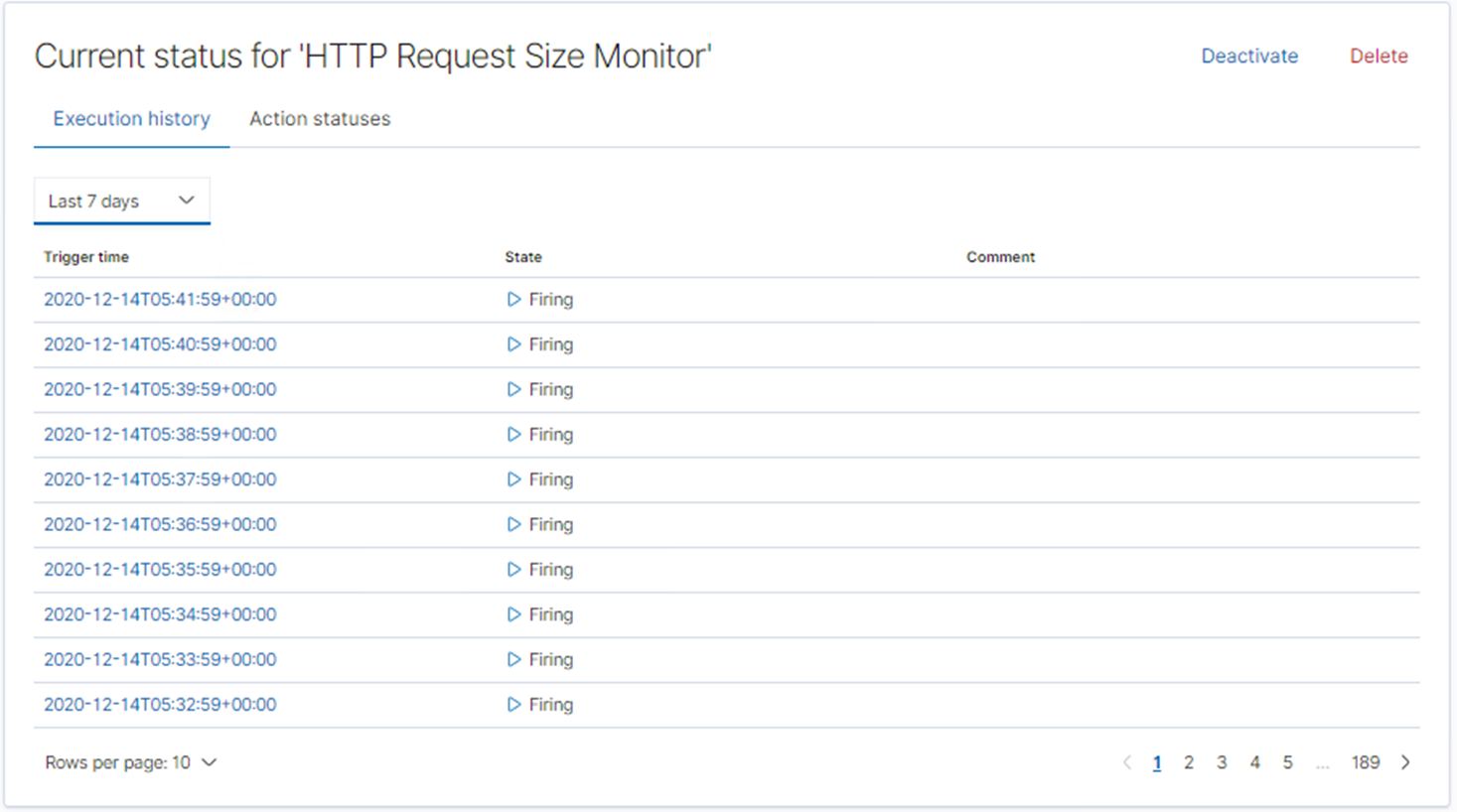
* This metric measures excessive HTTP errors such as 4xx and 5xx series errors
* The alert is instructed to run a watch every 5 minutes
* The alert sends a trigger when the the count is above 400 status response codes in a 5-minute window.



**Kibana Watcher Alert 3: HTTP requests size monitor**

**HTTP requests size Monitor** is implemented as follows:

* This metric measures the quantity of HTTP requests for documents
* The alert is instructed to run a watch every 1 minute
* The alert sends a trigger when the sum total of http requests for all documents is above 3500 requests in a 1-minute window.



## 

## **Suggestions for Going Further**

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

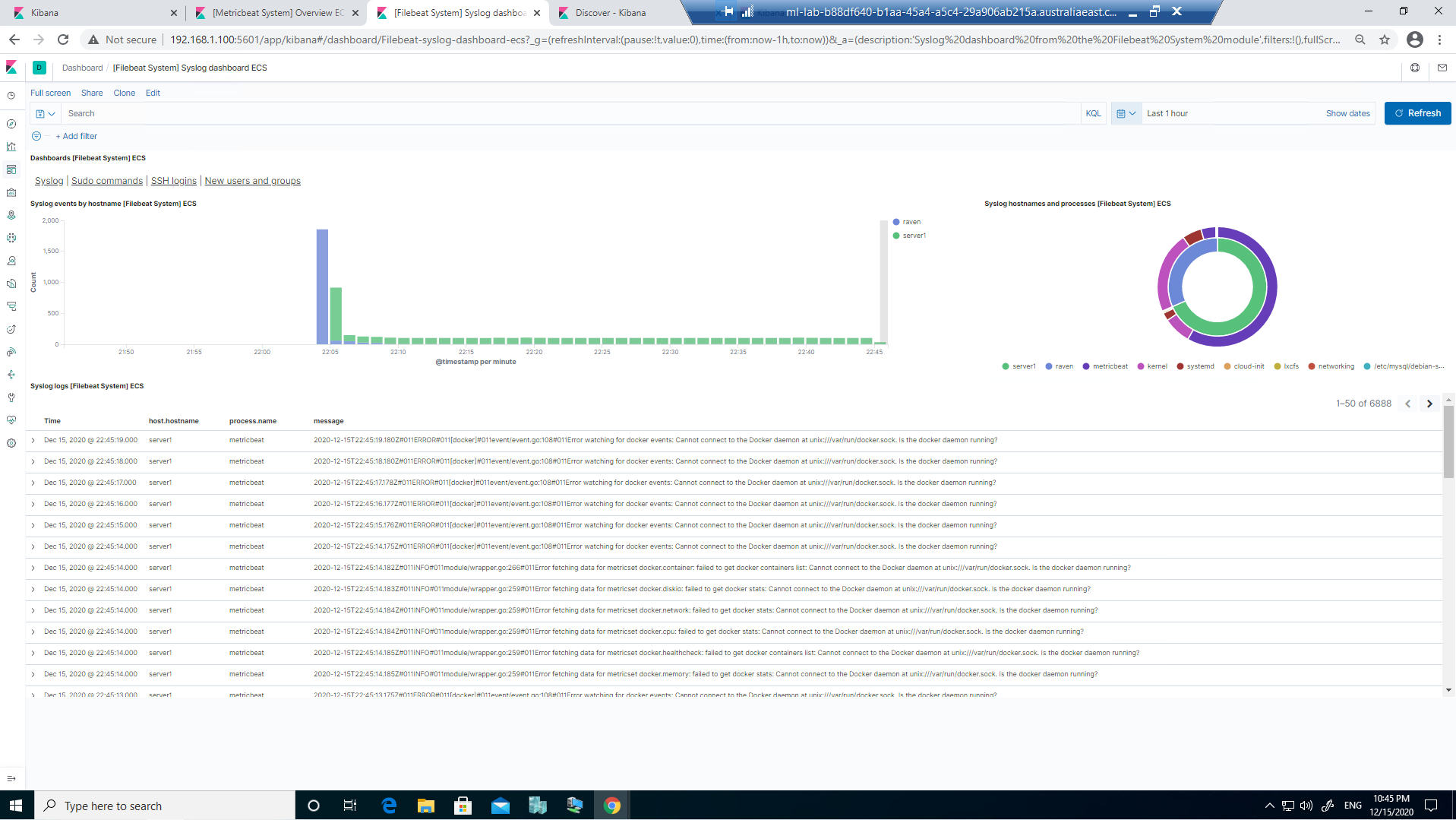
**Vulnerability: SSH Access**

* Patch: Upgrade your openssh to fix CVE-2016-0778
  + $ sudo apt-get update
  + $ sudo apt-get install openssh-client openssh-server openssh-sftp-server
* Why It Works: [For example: special-security-package scans the system for viruses every day]

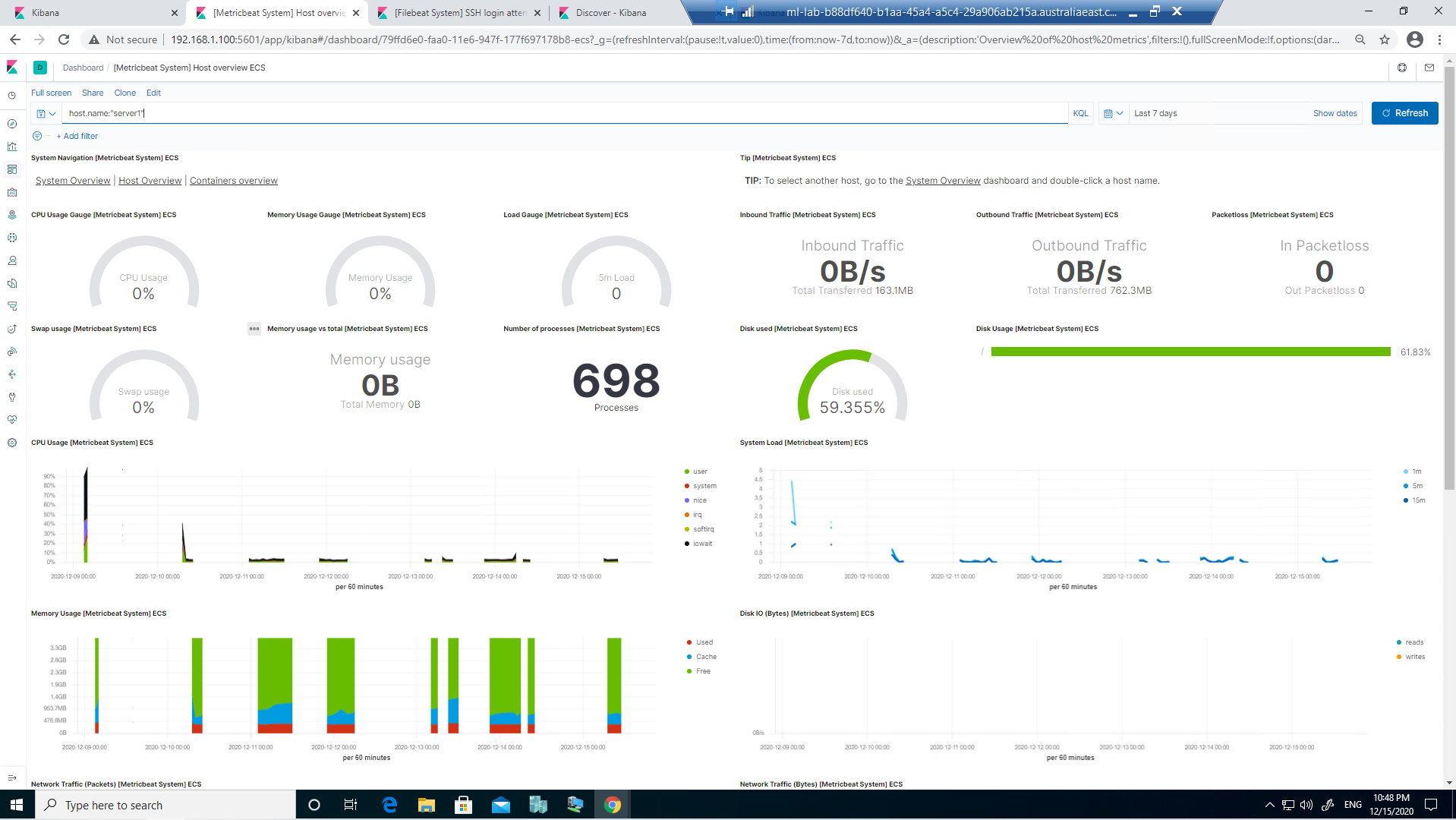
**Vulnerability: Wordpress out of date**

* Patch: <https://wordpress.org/support/article/updating-wordpress/#one-click-update> or <https://wordpress.org/download/>
* Why It Works: Updating all critical infrastructure and company software, including WordPress, should be done on a regular basis. Establish a policy whereby all company assets are checked for updates either weekly, fortnightly or monthly.

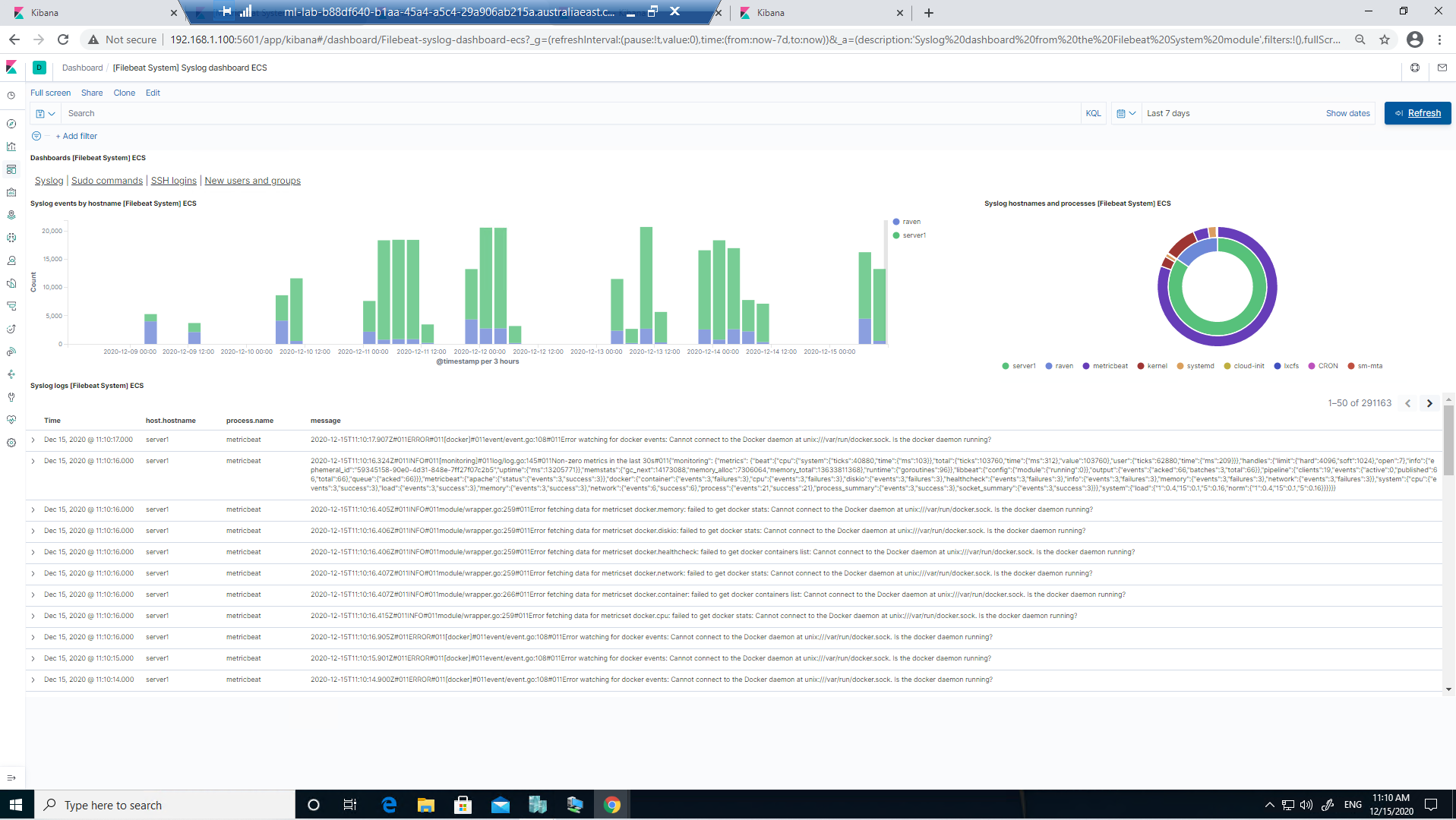
## **Screenshots Used As Evidence**



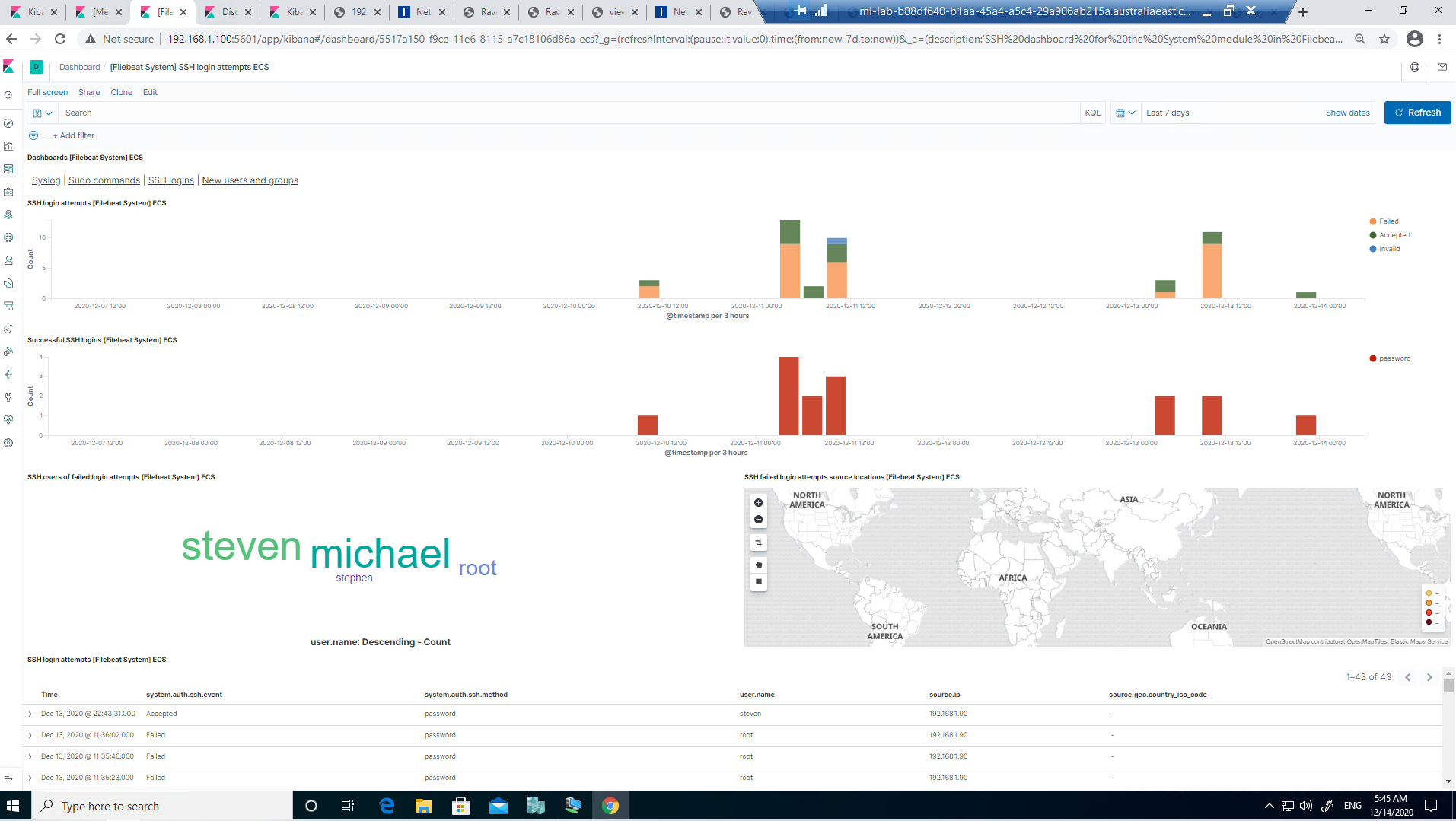
screenshot above: kibana (574)



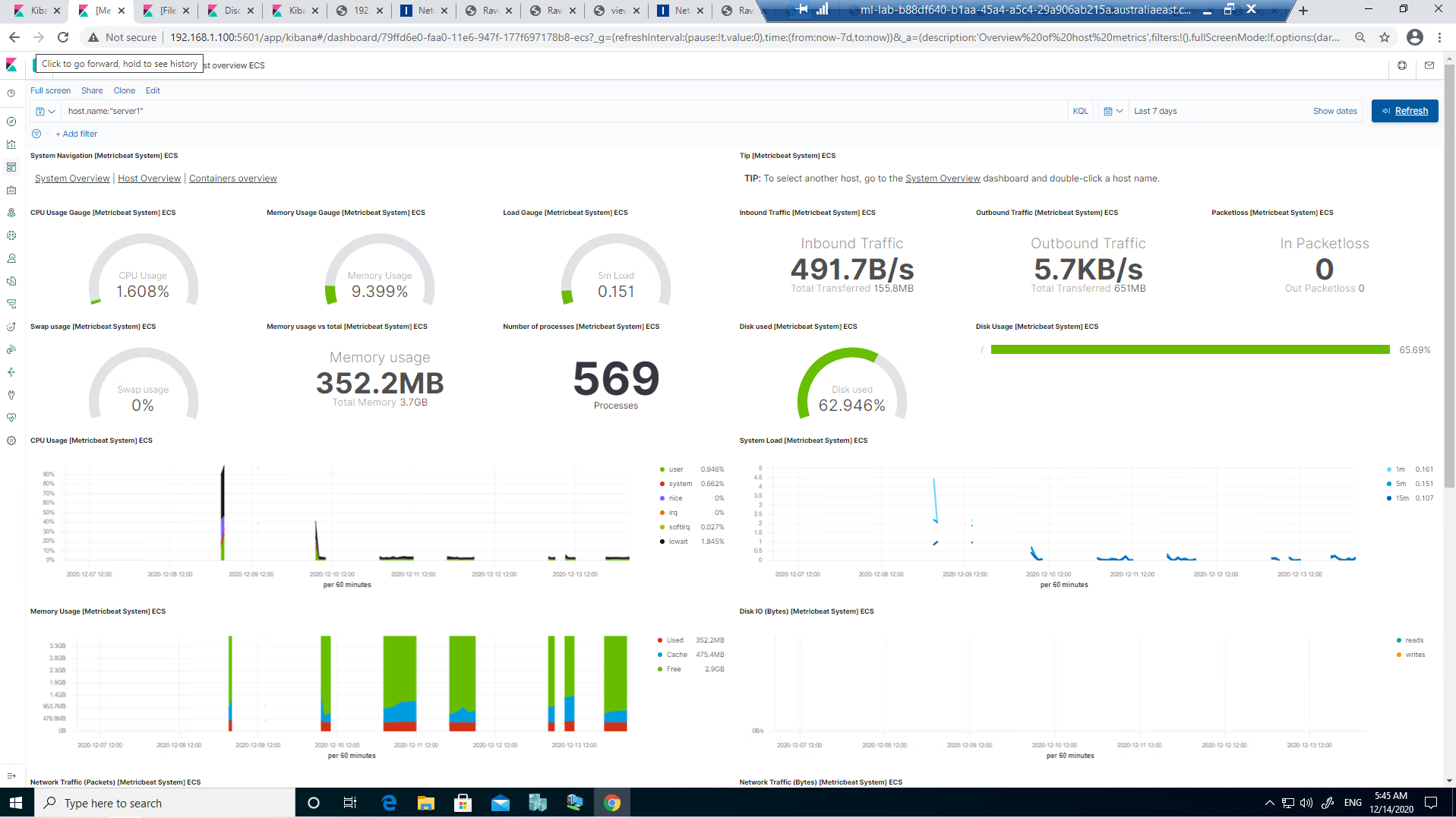
screenshot above: kibana (575)



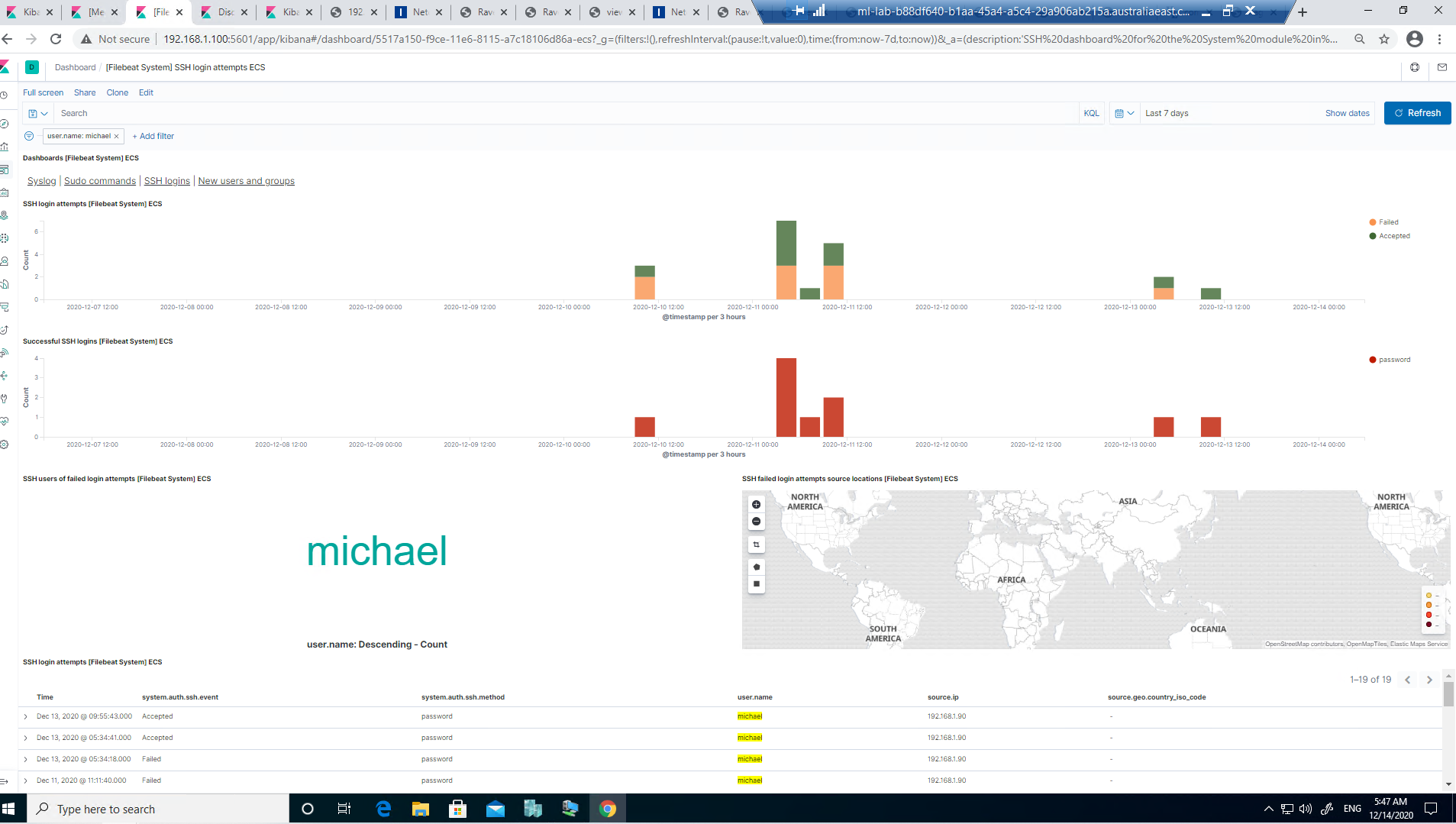
screenshot above: kibana\_7day\_syslog



screenshot above: kibana\_7days\_all\_SSH



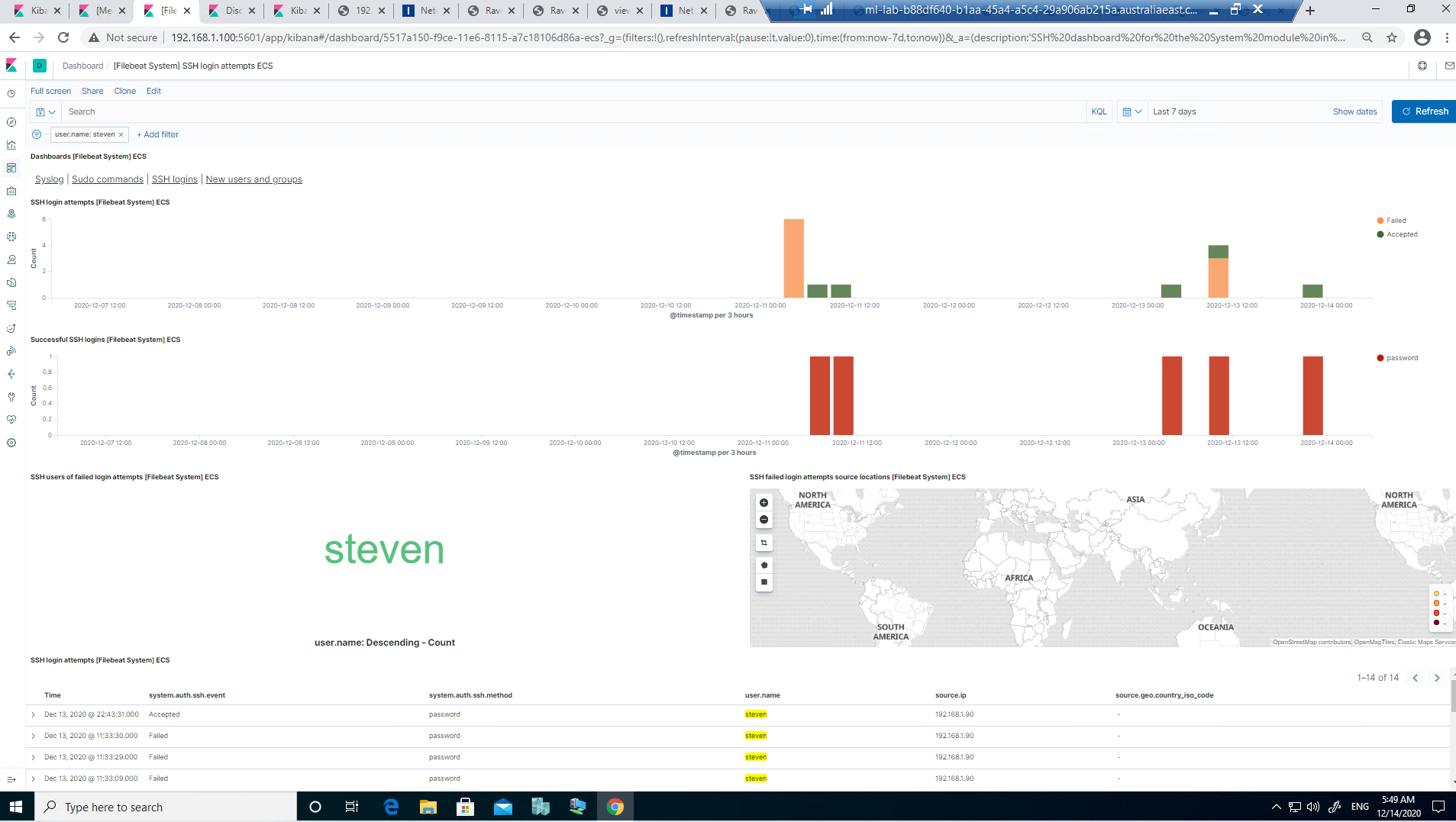
screenshot above: kibana\_7days\_host\_server1



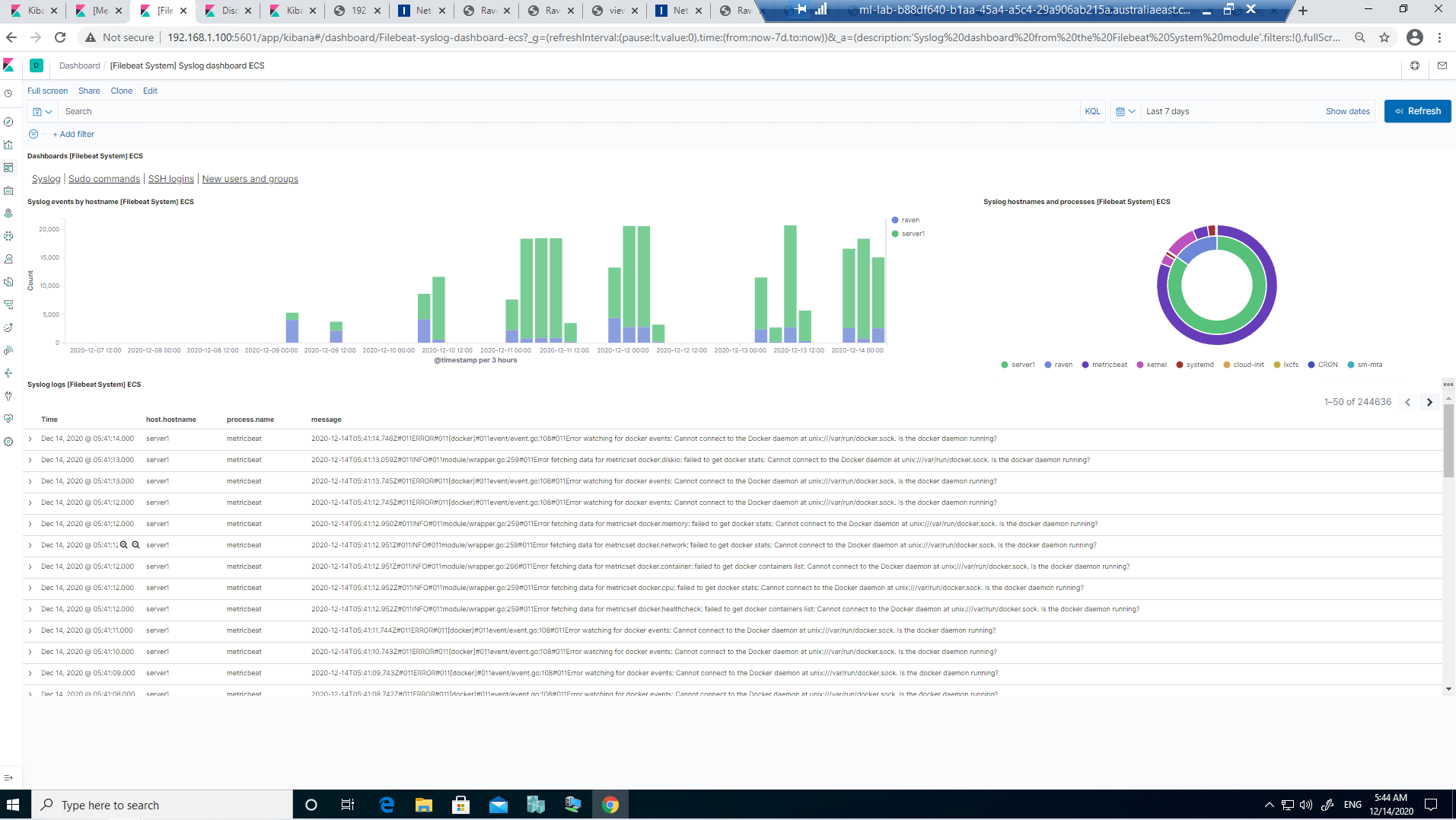
screenshot above: kibana\_7days\_michael



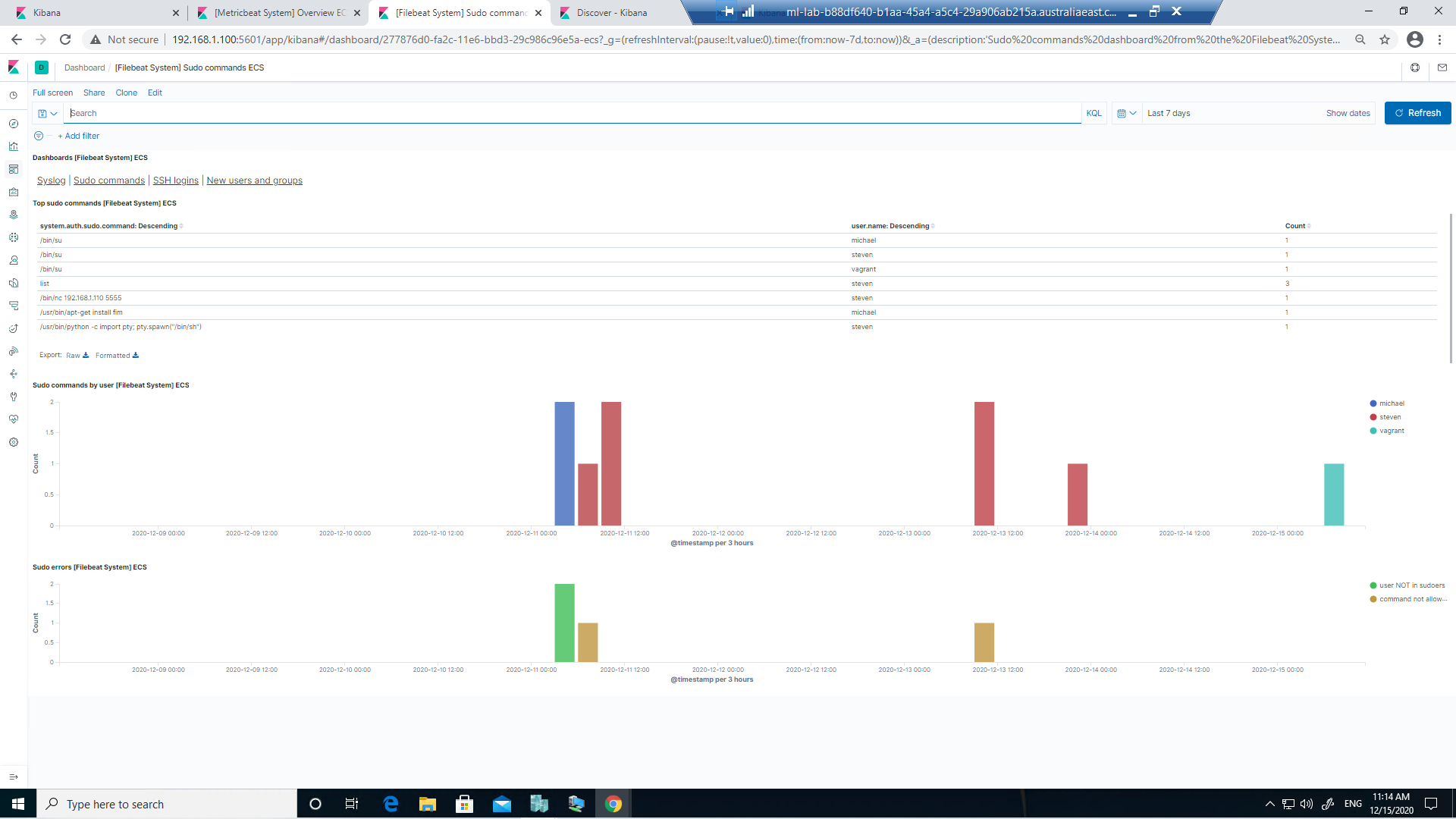
screenshot above: kibana\_7days\_packetbeat



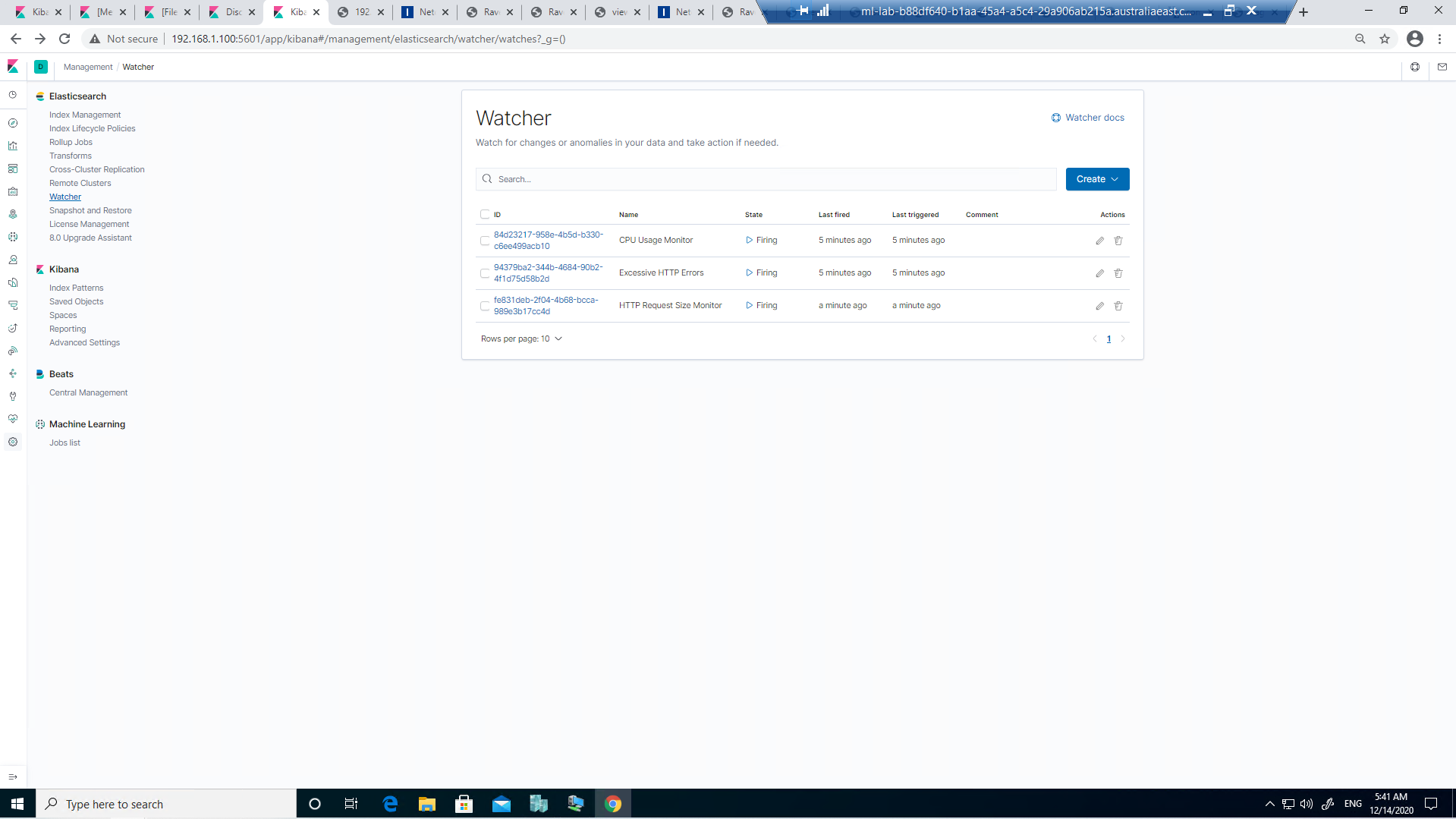
screenshot above: kibana\_7days\_steven



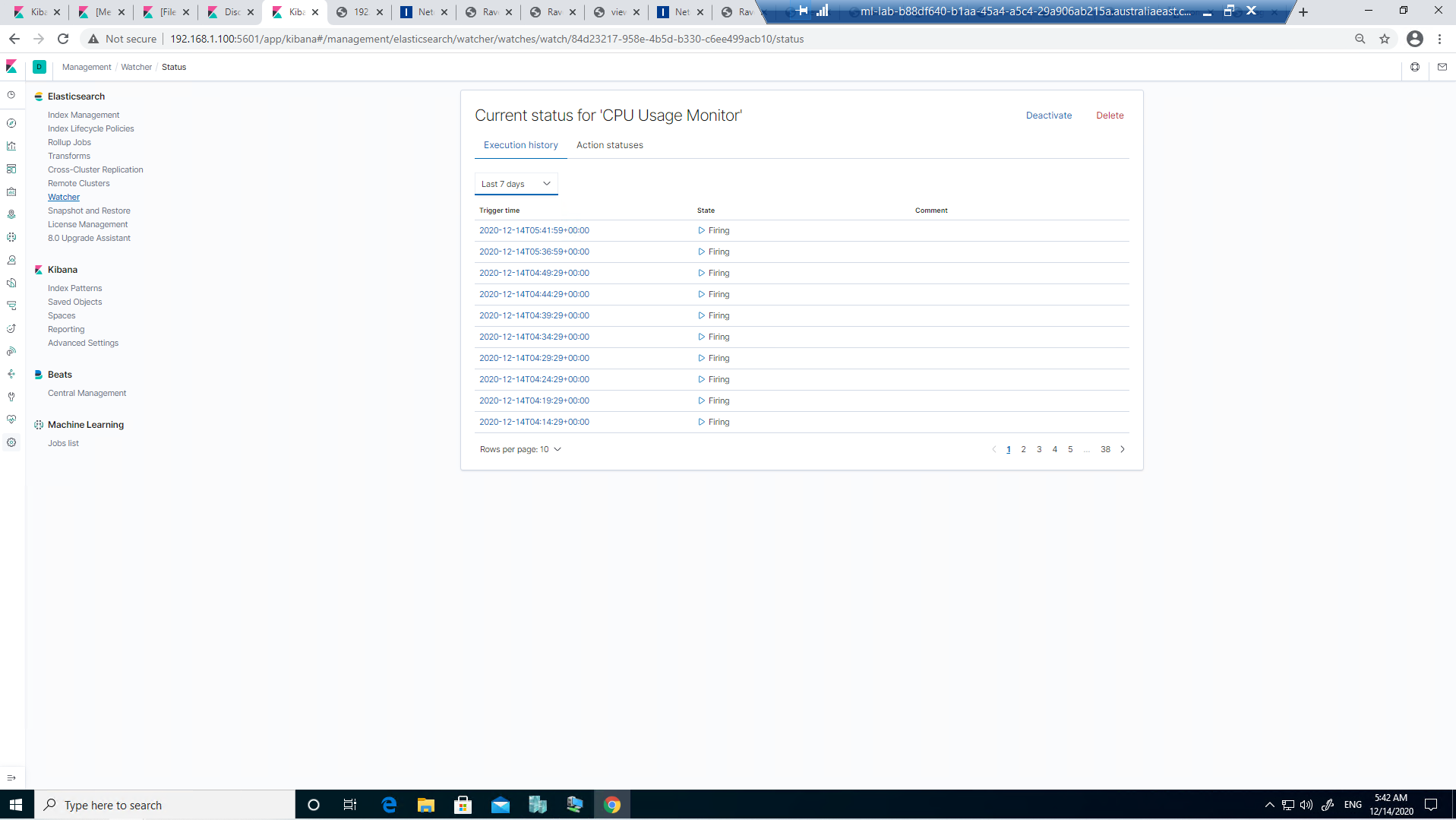
screenshot above: kibana\_7days\_syslog



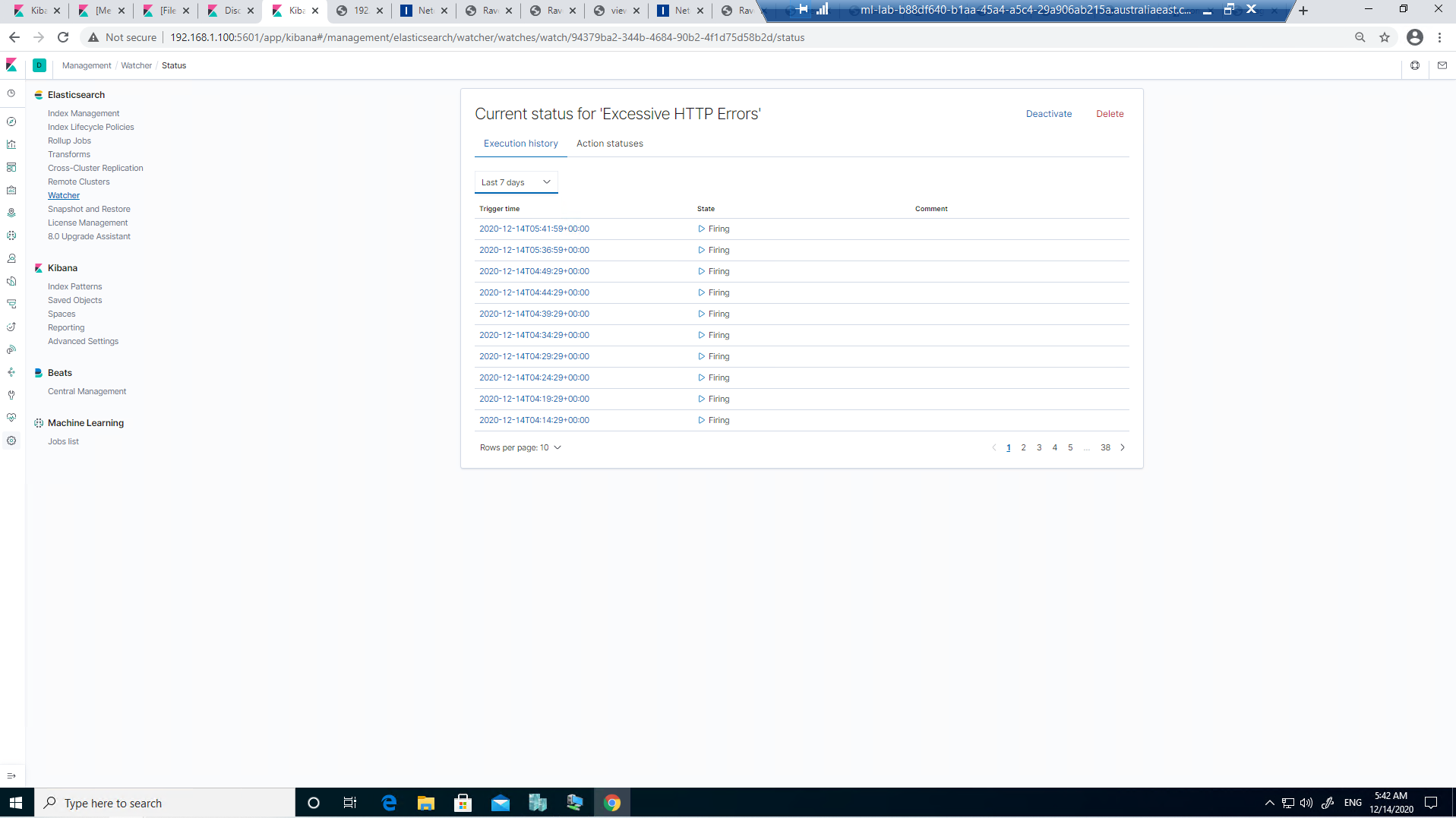
screenshot above: kibana\_target1\_7day\_user\_sudo



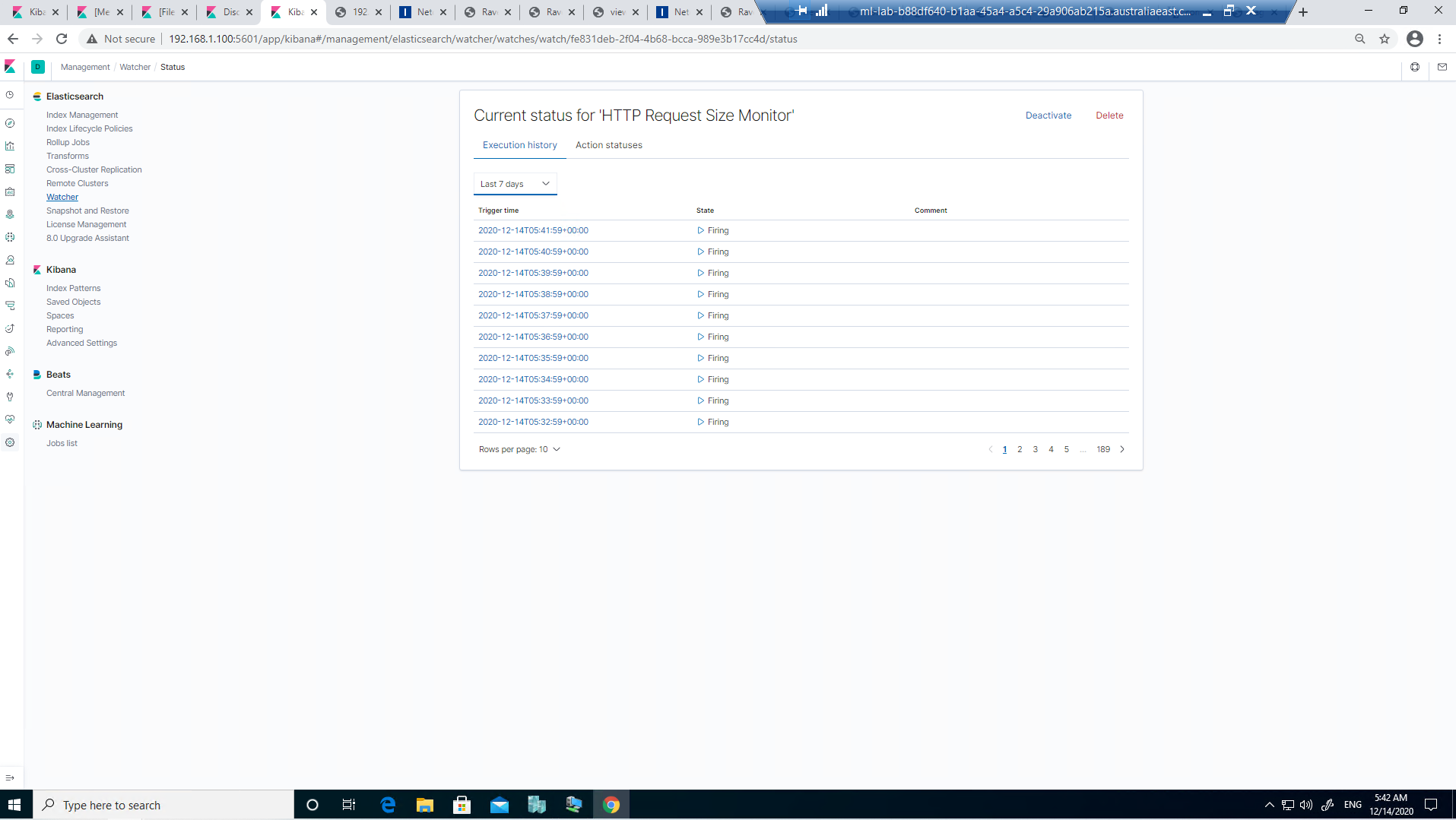
screenshot above: kibana\_watcher



screenshot above: kibana\_watcher\_CPU\_monitor



screenshot above: kibana\_watcher\_excessive\_http\_errors



screenshot above: kibana\_watcher\_excessive\_http\_errors