Activity File: Kibana Continued

- This week, you created the infrastructure behind a security information and event management system such as Kibana. Once that set up is complete, you will have finished the project.
- This optional activity tasks you with exploring more Kibana capabilities, some of which you will use in future projects.
- **Note**: In order to complete these activities, you will need to complete the optional Metricbeat configuration.

Scenario

In this activity, you will suppose the role of a cloud architect that has been tasked with setting up an ELK server to gather logs for the Incident Response team.

Before you hand over the server to the IR team, your senior architect has asked that you verify the ELK server is working as expected and pulling both logs and metrics from the pen-testing web servers.

You will have three tasks:

1. Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity.
2. Generate a high amount of CPU usage on the pen-testing machines and verify that Kibana picks up this data.
3. Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up.

These activities will guide you though generating some data to visualize in Kibana. Each of these activity will require the following high level steps:

1. Use your jump-box to attack your web machines in various ways.
2. Use a Linux utility to stress the system of a webVM directly.
3. Subsequently generate traffic and logs that Kibana will collect.

4. View that traffic in various ways inside Kibanna.

It's also worth noting that these activities comprise different job roles:

- Getting the infrastructure setup and maintaining it is the role of a security engineer or cloud architect.
- Using that infrastructure by creating dashboards and alerts fall under the security analyst role. It would be rare to have a position where you would be required to do both.

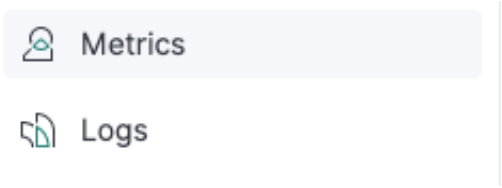
That said, now that we have Kibana setup and gathering data from three web servers, its worth learning how to visualize data in Kibana.

Before getting started, we'll have to complete some metrics and logs set up.

Setup: Kibana Metrics and Logs Orientation

Before we begin generating traffic, locate the two screens inside Kibana that you will use to visualize this traffic:

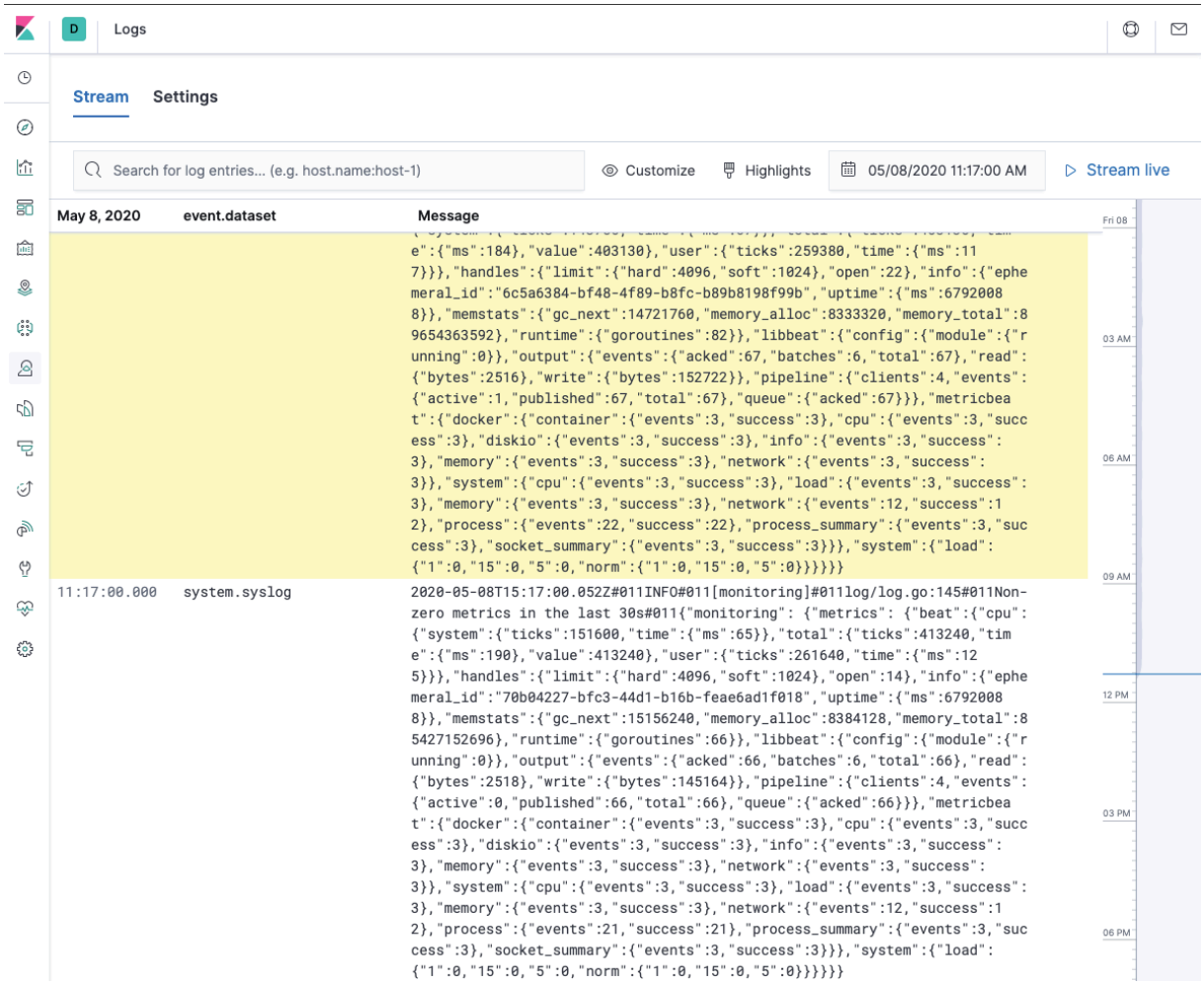
- Logs
- Metrics



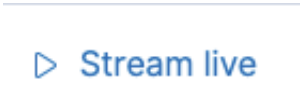
These pages will show you the changes in data that we will create.

Logs

- Click **Logs** to see some general system logs coming from the web machines.



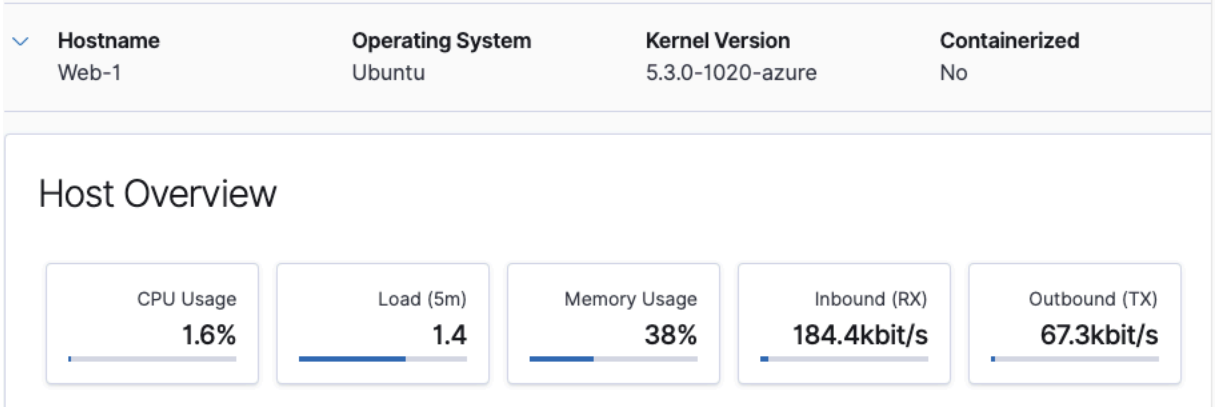
- Notice that you can stream logs live from the machines.



Metrics

- Next, click **Metrics** on the left side.
    - Here we can see each of our VMs that are sending metrics.
- Click on one of the large squares that represent one of your VMs.
- Choose **View metrics** from the dropdown that appears.

- Notice that you can see CPU and memory usage here.



Now that we know where to look for this data, let's generate some unusual network traffic.

Activity Tasks

Expand the provided activity files to complete each task. These tasks can be completed in any order.

SSH Barrage

Task: Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity.

- Activity File: SSH Barrage

Linux Stress

Task: Generate a high amount of CPU usage on the pentesting machines and verify that Kibana picks up this data.

- Activity File: Linux Stress

wget-DoS

Task: Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up.

- Activity File: wget-DoS
