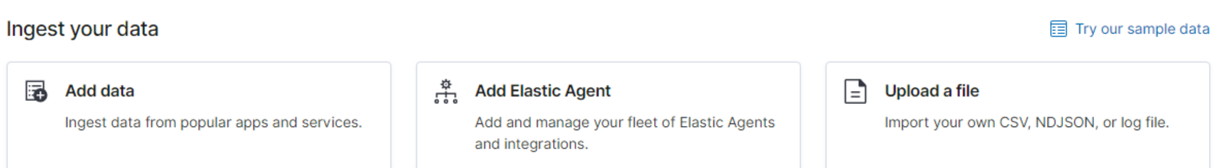
Kibana Implementation Suggestions

Produced for CISA by Team Anomalous

Kibana Capabilities Utilized

Within your Elastic Deployment, you will open the Kibana section which is also known as ‘Analytics’. There were four subcomponents used within Kibana which were: Discover, Dashboard, Machine Learning, and Visualize Library. There are two methodologies to ploading a dataset into your deployment. These are ingested via Logstash or uploading the dataset. In our use case, the small datasets on The Mordor Project were small enough to upload the dataset file. This can be found on the “Home” page of your Elasticdeployment.



For larger datasets like the APT 29, you will need to utilize the capabilities of Logstash to ingest the dataset into your deployment. Steps for ingesting via Logstash are provided in our other supplementary Technical Guides.

Discover:

Within Kibana, Discover allows you to quickly search and filter through your datasets. You can explore your dataset by conducting queries. Additionally, when a dataset is uploaded or ingested there will be different key ‘fields’ available to choose from to continue breaking down the dataset.

Dashboard:

After you have parsed through your data and found key things you want to be visualized, you can then save those visualizations and import them into a dashboard. A dashboard brings all of the visualizations created in one place for a user, in our project these dashboards were created in the mind of a SOC analyst viewpoint.

Machine Learning:

Parsing through small datasets consisting of 15 minutes of a data stream is a lot easier to conduct analysis and find anomales within. Analyzing a larger dataset like the APT 29 dataset, it becomes a lot more challenging to conduct manual analysis for anomalies. The Machine Learning section of Kibana can be leveraged to utilize its anomaly detection and outlier detection. Furher instructions for setting up Machine Learning jobs can be found in our supplementary guide.

Visualize Library:

This is the section where you can begin creating visualizations of different fields within a dataset. On the left-hand side, click on the three horizontal lines and then click on 'Visualize Library'. Click: 'Create Visualization'. For our project, we used the 'Lens' feature. You will then want to change your dataset aka index to the one you want to make a visualization for. **Note:** Make sure to re-adjust the data range to encompass the dataset → this is found in the top right -hand corner. You will then click and drag a field into the center box where it will then begin creating a visualization. Kibana will showcase a suggested visualization as well as previews for other visualization suggestions below. On the right-hand side, there is a section where you can adjust the visualization to adjust things like color, a number of values to showcase, rank direction, etc. Then save the visualization in the top right-hand corner. Add it to a dashboard upon saving or to your visualization library which can be accessed when in the 'Visualize Library'.

Step by step guide:

1. In the top left corner of your deployment, click the three horizontal bars
2. Click 'Visualize Library'
3. Click 'Create Visualization'
4. Select option for visualization
    a. We utilized 'Lens'
5. Change dataset/index which is found in the bar with the drop-down arrow
6. Adjust data range in the top right-hand corner
7. Drag and drop a field into the center
8. A visualization suggestion will be prepopulated
9. Adjust visualization accordingly
10. Save the visualization
    a. You can immediately add it to a dashboard upon saving or add it to the library
    b. As well as create and tag a visualization i.e. to differentiate between different datasets