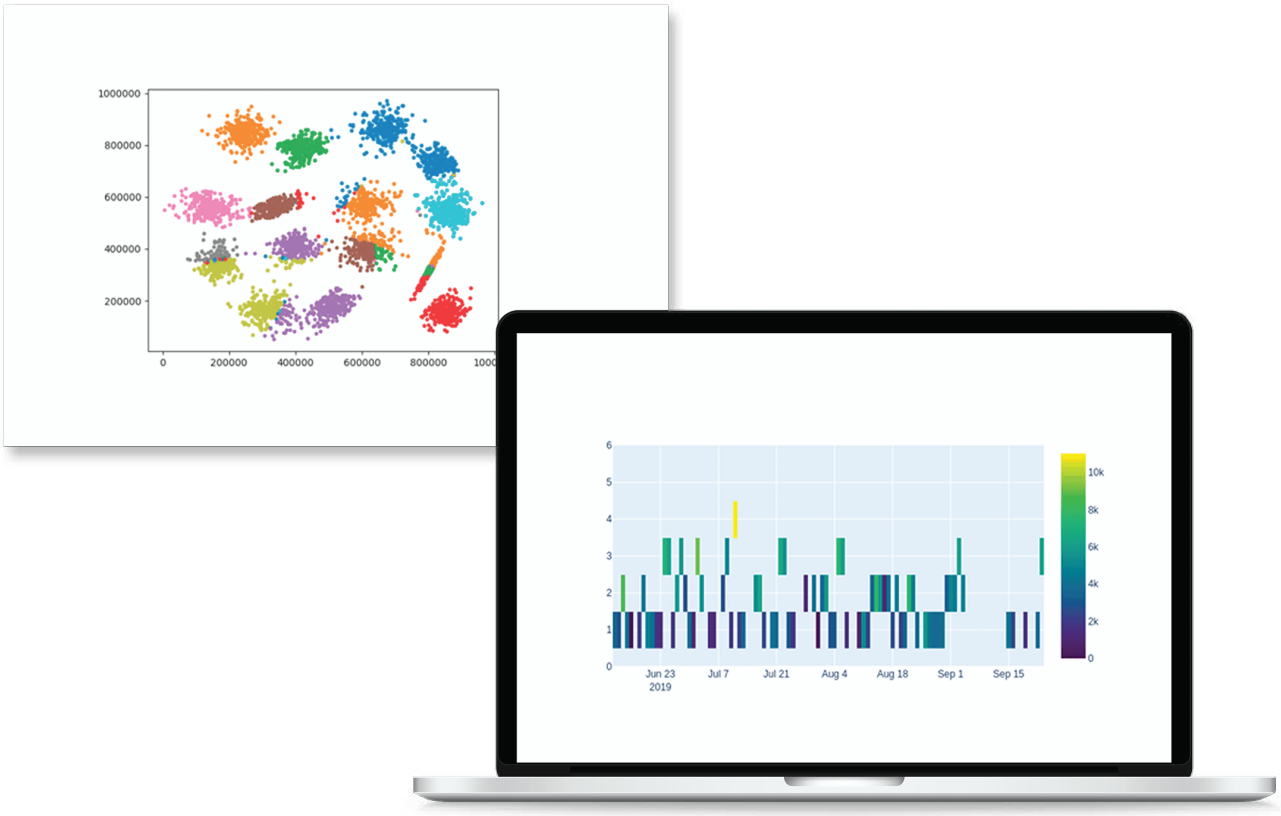
B-have
advanced **anomaly detection**

B-Have is a library oriented to the processing and analysis of data patterns using Machine Learning algorithms. In particular, this library allows applying data cluster, deep learning, reinforcement learning, and temporal dissection for traffic and event anomaly detection and attack classification

Applications

- Bayesian based anomaly detection
- Temporal pattern learning for attack classification
- Convolutional learning for matrix represented data
- Geometrical clustering Spectral clustering



powered by: vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Use cases

Application includes:

- Network traffic anomaly detection
- Behaviour Attack classification
- Spectrogram based anomaly detection
- Network device clustering
- Temporal Spectrogram based anomaly detection
- Industrial event prediction

Architecture

Bhave consist of two parts: the clustering part and the detection/classification part.

In the first one, clustering modules can be found, while detection/classification modules are contained in the second one.

Input data follows a generic structure for all detection algorithms, for the easing of the user when analyzing data.

Module	Description	Dependencies	Languaje
bayesian_learning	Bayesian based detection/classification	Statsmodels, scicpy, numpy	Python 3.7
convolutional_learning	Convolutional based detection/classification	Numpy, pandas, tensorflow	
temporal_learning	Temporal based detection/classification	Numpy, pandas, tensorflow	
general_learning	More general algorithms for detection/classification	Numpy, pandas, tensorflow	
graph_clustering	Spectral clustering	Pandas, numpy	

Contact Us

www.vicomtech.org tech.transfer@vicomtech.org +34 943 309 230

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE