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
**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.

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>Dependencies</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>bayesian_learning</td>
<td>Bayesian based detection/classification</td>
<td>Statsmodels, scipy, numpy</td>
<td></td>
</tr>
<tr>
<td>convolutional_learning</td>
<td>Convolutional based detection/classification</td>
<td>Numpy, pandas, tensorflow</td>
<td></td>
</tr>
<tr>
<td>temporal_learning</td>
<td>Temporal based detection/classification</td>
<td>Numpy, pandas, tensorflow</td>
<td></td>
</tr>
<tr>
<td>general_learning</td>
<td>More general algorithms for detection/classification</td>
<td>Numpy, pandas, tensorflow</td>
<td></td>
</tr>
<tr>
<td>graph_clustering</td>
<td>Spectral clustering</td>
<td>Pandas, numpy</td>
<td>Python 3.7</td>
</tr>
</tbody>
</table>