AD is a SPHINX component, which is based on both machine learning and statistics-based algorithms. It performs a fast and efficient analysis of the network packets and detects unknown attacks. The ID dashboard for Anomaly detection displays relevant data about AD alerts, filtered by an algorithm type (VerticalPortScan, UDPAmplifier, SMTPTalker, P2PCommunication, MediaStreamingClient, ICMPTunnel, HorizontalPortScan, DnsTunnel, CCBotNet, AtypicalTCPPortUsed, AtypicalNumberOfPairs, AtypicalAmountData, AtypicalAlienTCPPortUsed, AlienAccessingManyHosts and AbusedSMTP) that can be choosed by the user in the top left corner of the dashboard.

Visualisations:

- Number of alerts today;
- Number of alerts yesterday;
- Number of alerts two days ago;
- Number of alerts per day graph;
- Logs (containing detailed data about AD).